

Kaspersky Anti-Virus 8.0 for Lotus Domino

KASPERSKY **lab**

Guide de l'administrateur

VERSION DE L'APPLICATION: 8.0

Chers utilisateurs !

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

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (puis dans le texte Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois de la France.

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

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

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

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

Ce document reprend des marques commerciales et des marques de service qui appartiennent à leurs propriétaires respectifs.

Date d'édition du document : 19.11.2010

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

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

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À ÊTRE LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTÉZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

SI UN CONTRAT DE LICENCE OU UN DOCUMENT SIMILAIRE ACCOMPAGNE LE LOGICIEL, LES CONDITIONS D'UTILISATION DU LOGICIEL DÉFINIES DANS CE DOCUMENT PRÉVALENT SUR LE PRÉSENT CONTRAT DE LICENCE D'UTILISATEUR FINAL.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

- 1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.
- 1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.
- 1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.
- 1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, " Vous " signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme " entité ", sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.
- 1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.
- 1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patches, les modifications, les copies, les ajouts ou les packs de maintenance, etc.
- 1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

- 2.1. Une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (" l'utilisation ") du Logiciel sur un nombre spécifié d'Ordinateurs vous est octroyée pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la " Licence "), et vous acceptez cette Licence :
Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel

de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs précisés dans les licences que vous avez obtenues, *sachant que*, sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

- 2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.
- 2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.
- 2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.
- 2.5. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :
 - Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
 - Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

- 3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.
- 3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.
- 3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.
- 3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.
- 3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.
- 3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.
- 3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence sans rembourser le prix d'achat en tout ou en partie.
- 3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.
- 3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

- 4.1. L'assistance technique décrite dans la Clause 2.5 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : <http://support.kaspersky.com>
- 4.2. Les données de l'utilisateur, spécifiées dans Personal Cabinet/My Kaspersky Account, ne peuvent être utilisées par les spécialistes de l'assistance technique que lors du traitement d'une requête de l'utilisateur.

5. Limitations

- 5.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.
- 5.2. Vous ne devez transférer les droits d'utilisation du Logiciel à aucune tierce partie.
- 5.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits.
- 5.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.
- 5.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.
- 5.6. Votre fichier clé peut être bloqué en cas de non-respect de Votre part des conditions générales de ce Contrat.
- 5.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

6. **Garantie limitée et avis de non-responsabilité**

- 6.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément déchargé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.
- 6.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adapté à Votre cas.
- 6.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.
- 6.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.5 de ce Contrat.
- 6.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.
- 6.6. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PAR LA LÉGISLATION EN VIGUEUR, LA " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

7. **Exclusion et Limitation de responsabilité**

- 7.1. DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET/OU DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS ET/OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SOIT LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

8. Licence GNU et autres licences de tierces parties

- 8.1. Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

9. Droits de propriété intellectuelle

- 9.1. Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des États-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur

le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

9.2. Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

10. Droit applicable ; arbitrage

10.1. Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations-Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 10 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

11. Délai de recours.

11.1. Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

12. Intégralité de l'accord ; divisibilité ; absence de renoncement.

12.1. Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en équité de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

13. Informations de contact du Titulaire des droits

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. : +7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Tous droits réservés. Les marques commerciales et marques de service déposées appartiennent à leurs propriétaires respectifs.

CONTENU

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB.....	3
PRÉSENTATION DU GUIDE	11
Dans ce document.....	11
Conventions.....	13
SOURCES COMPLÉMENTAIRES D'INFORMATIONS SUR L'APPLICATION	14
Sources d'informations pour une aide autonome.....	14
Contacter le service commercial.....	15
Communication avec le Groupe de rédaction de la documentation technique	15
Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne	15
KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO	16
Nouveautés.....	17
Distribution.....	18
Service pour les utilisateurs enregistrés	18
Configurations logicielle et matérielle.....	18
ARCHITECTURE DE L'APPLICATION	20
Schéma de la protection antivirus du serveur.....	21
Schéma de fonctionnement de l'application	22
Algorithme de la recherche d'éventuelles menaces dans les objets	23
Algorithme de filtrage des pièces jointes	23
Traitement des objets et actions exécutées sur ceux-ci.....	24
Administration des paramètres de Kaspersky Anti-Virus.....	24
Administration des paramètres du fichier de configuration notes.ini	26
Administration des privilèges	28
Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus.	28
Privilèges des groupes fonctionnels	29
Octroi de privilèges des groupes fonctionnels aux utilisateurs	30
Administration des privilèges au niveau des paramètres du profil/serveur.....	31
ADMINISTRATION DES LICENCES.....	32
Présentation du contrat de licence.....	32
Présentation des licences de Kaspersky Anti-Virus.....	33
Présentation des fichiers de licence de Kaspersky Anti-Virus	33
Installation du fichier de licence	34
INTERFACE DE L'APPLICATION.....	36
Structure de la fenêtre de la base de données Centre d'administration.....	38
Onglet Administration de la protection	39
Onglet Journal des événements et statistiques	42
Onglet Aide.....	43
LANCEMENT ET ARRÊT DE L'APPLICATION	44
ÉTAT DE LA PROTECTION DU SERVEUR	45
PROTECTION DU SERVEUR PAR DÉFAUT	47
MISE À JOUR DES BASES	49
Source des mises à jour	50

Schémas de mise à jour	51
Sélection de la source de mises à jour	53
Mise à jour selon la programmation	54
Mise à jour manuelle	56
PROTECTION DU COURRIER	57
Activation et désactivation de la protection du courrier	58
Sélection des objets pour la protection du courrier	59
Actions à exécuter sur les objets du courrier	60
Filtrage des pièces jointes du courrier	64
Notifications sur les épidémies	66
PROTECTION DES RÉPLICATIONS	69
Activation/désactivation de la protection des répliques	70
Sélection des objets de la protection des répliques	71
Actions à exécuter sur les objets en mode de protection des répliques	72
Filtrage des pièces jointes en mode de protection des répliques	74
ANALYSE DES BASES DE DONNÉES	76
Activation et désactivation de l'analyse des bases de données	77
Sélection des objets à analyser des bases de données	78
Actions à exécuter sur les objets en mode d'analyse des bases de données	80
Filtrage des pièces jointes en mode d'analyse des bases de données	82
Analyse selon la programmation	84
Analyse manuelle	85
PRODUCTIVITÉ	86
QUARANTAINE	88
Consultation des objets placés en quarantaine	88
Actions à exécuter sur les objets placés en quarantaine	91
Configuration de la quarantaine	93
JOURNAL DES ÉVÉNEMENTS ET STATISTIQUES	95
Configuration des paramètres du journal des événements	96
Configuration des paramètres des statistiques	98
Suppression des informations de la base de données Journal des événements et statistiques	101
Consultation de la base de données Journal des événements et statistiques	102
Consultation du journal global des événements et des statistiques	102
Journal des événements	103
Statistiques	103
Consultation du journal des événements et des statistiques pour le serveur	105
NOTIFICATIONS	106
ADMINISTRATION DE LA CONFIGURATION	109
Création et suppression de profils	109
Désignation de l'administrateur de profil	111
Désignation de l'administrateur de serveur	111
Déplacement du serveur vers un autre profil	112
Définition de valeurs individuelles pour les paramètres du serveur	112
Exploitation de la possibilité de modification directe des paramètres du serveur	114
VALIDATION DE LA CONFIGURATION DE L'APPLICATION	116
Virus d'essai EICAR et ses modifications	116

Test de la protection du courrier	117
Test de la protection des répliquions.....	118
Test de l'analyse des bases de données	118
UTILISATION VIA LA CONSOLE DU SERVEUR	119
CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE	121
GLOSSAIRE.....	122
KASPERSKY LAB.....	124
INFORMATIONS SUR LE CODE TIERS	125
Code logiciel	125
BOOST 1.30.....	125
EXPAT 1.2	125
GECKO SDK 1.8.....	125
INFO-ZIP 5.51.....	134
LIBNKF 2.0.5.....	135
LZMA SDK 4.43	135
OPENSSL 0.9.8D.....	135
PCRE 7.4	137
RFC1321-BASED (RSA-FREE) MD5 LIBRARY	138
ZLIB 1.2.....	138
Outils de développement	138
AUTOCONF 2.61	138
AUTOMAKE 1.10	138
AWK 3.1.5.....	138
BASH 3.2.33	138
GCC 4.1.2	139
GCC 3.4.5	139
GCC 3.3.6	139
GCC 3.3.2	139
GNU MAKE 3.81	140
GREP 2.5.1	140
PERL 5.8.8.....	140
SED 4.1.5.....	142
Informations diverses.....	142
GNU GENERAL PUBLIC LICENSE.....	142
INDEX	163

PRÉSENTATION DU GUIDE

L'équipe de spécialistes de Kaspersky Lab vous souhaite la bienvenue. Nous espérons que les informations fournies dans ce guide vous aideront à utiliser Kaspersky Anti-Virus for Lotus Domino.

Les informations relatives à l'installation de Kaspersky Anti-Virus sont reprises dans le Guide de déploiement.

Le guide est destiné aux administrateurs de réseaux d'entreprise. Il contient des informations sur l'utilisation de l'application, sur la configuration des paramètres, sur l'administration de la protection d'un serveur ou d'un groupe de serveurs via le client Lotus, via l'interface Web de l'application ou via la console de serveur Domino.

Si vous ne trouvez pas la réponse à vos questions sur Kaspersky Anti-Virus dans ce document, vous pouvez consulter d'autres sources d'informations sur Kaspersky Anti-Virus.

DANS CETTE SECTION

Dans ce document.....	11
Conventions	13

DANS CE DOCUMENT

Les sections suivantes sont présentées dans ce document :

- *Texte du contrat de licence* (cf. page [3](#)). Cette rubrique présente le texte du contrat de licence entre Kaspersky Lab et l'utilisateur final qui octroie les droits et définit les restrictions sur l'utilisation de Kaspersky Anti-Virus 8.0 for Lotus Domino.
- *Sources complémentaires d'informations sur l'application* (cf. page [14](#)). Cette rubrique fournit des informations sur les sources d'informations relatives à l'application autres que les documents fournis avec la distribution et explique comment contacter Kaspersky Lab pour obtenir les renseignements requis.
- *Kaspersky Anti-Virus 8.0 for Lotus Domino* (cf. page [16](#)). Cette rubrique reprend les principales fonctionnalités de Kaspersky Anti-Virus 8.0 for Lotus Domino, les différences entre cette version de l'application et la version antérieure, ainsi que la configuration minimale requise pour l'ordinateur sur lequel Kaspersky Anti-Virus sera installé et utilisé.
- *Architecture de l'application* (cf. page [20](#)). Cette rubrique 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 et sur l'administration des privilèges des utilisateurs.
- *Administration des licences* (cf. page [32](#)). Cette rubrique fournit des informations détaillées sur les notions fondamentales liées aux licences de Kaspersky Anti-Virus et explique également comment installer et supprimer la licence pour Kaspersky Anti-Virus.
- *Interface de l'application* (cf. page [36](#)). Cette rubrique décrit les principaux éléments de l'interface 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 [44](#)). Cette rubrique explique comment lancer et arrêter Kaspersky Anti-Virus sur le serveur et décrit la procédure de connexion au serveur pour configurer les paramètres de l'application.
- *État de la protection du serveur* (cf. page [45](#)). Cette rubrique explique comment consulter les informations relatives à la protection antivirus du serveur via l'interface de Kaspersky Anti-Virus : quels sont les composants

de la protection qui sont activés ou désactivés et comment activer ou désactiver les composants de la protection antivirus du serveur.

- *Protection par défaut du serveur* (cf. page [47](#)). Cette rubrique 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 [49](#)). Cette rubrique explique comment configurer les paramètres de la mise à jour des bases antivirus aussi bien pour un serveur que pour un groupe de serveurs, quels sont les sources de mise à jour qui peuvent être utilisées et comment lancer la mise à jour des bases antivirus manuellement et selon une programmation. La rubrique offre également des informations sur le modèle de mise à jour de Kaspersky Anti-Virus dans le contexte d'une installation sur un serveur ou sur plusieurs.
- *Protection du courrier* (cf. page [57](#)). Cette rubrique explique comment activer ou désactiver la protection du courrier pour le serveur Domino, comment sélectionner les objets des messages à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des messages en fonction des résultats de l'analyse et comment configurer les notifications sur les épidémies.
- *Protection des répliquions* (cf. page [69](#)). Cette rubrique explique comment activer ou désactiver la protection des répliquions, comment choisir les objets des répliquions à analyser, comment configurer le filtrage des pièces jointes, comment configurer le traitement des objets des répliquions en fonction des résultats de l'analyse.
- *Analyse des bases de données* (cf. page [76](#)). Cette rubrique 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.
- *Productivité* (cf. page [86](#)). Cette rubrique décrit les paramètres qui définissent les performances de l'application et comment les configurer.
- *Quarantaine* (cf. page [88](#)). Cette rubrique fournit des informations sur la manière de consulter les objets placés en quarantaine, comment configurer le traitement des objets placés en quarantaine et comment configurer les paramètres de la quarantaine.
- *Journal des événements et statistiques* (cf. page [95](#)). Cette rubrique explique comment configurer le journal des événements et statistiques et comment consulter la base de données Journal des événements et statistiques.
- *Notifications* (cf. page [106](#)). Cette rubrique décrit comment configurer les paramètres des notifications sur les objets découverts lors de l'analyse.
- *Administration des configurations* (cf. page [109](#)). Cette rubrique explique comment ajouter ou supprimer des profils, comment déplacer un serveur dans un autre profil et comment configurer les paramètres du serveur.
- *Validation de la configuration de l'application*. Cette rubrique explique comment vérifier l'exactitude de la configuration des paramètres pour chaque composant de la protection à l'aide du virus d'essai eicar et de ses modifications.
- *Utilisation via la console du serveur* (cf. page [119](#)). La rubrique décrit les instructions pour l'administration de Kaspersky Anti-Virus via la ligne de commande dans la console du serveur Domino.
- *Contacter le service d'assistance technique* (cf. page [121](#)). Cette rubrique explique les règles à suivre pour contacter le service d'assistance technique.
- *Glossaire* (cf. page [122](#)). Cette rubrique fournit la définition des termes utilisés dans ce guide.
- *Kaspersky Lab* (cf. page [124](#)). Cette rubrique fournit des informations sur Kaspersky Lab.
- *Informations sur l'utilisation de code tiers* (cf. page [125](#)). Cette rubrique fournit des informations sur le code tiers utilisé dans l'application.

CONVENTIONS

Les conventions reprises dans le tableau ci-dessous sont utilisées dans ce guide.

Tableau 1. Conventions

TYPE D'INFORMATION	CONVENTION
N'oubliez pas que...	Texte d'un avertissement.
Il est conseillé d'utiliser...	Texte d'une remarque.
Exemple : ...	Texte d'un exemple.
CTRL+SHIFT	Noms des touches du clavier.
Activer	Nom d'un élément de l'interface.
<i>Mise à jour</i>	Nouveau terme.
➡ <i>Pour planifier une tâche, procédez comme suit :</i>	Texte d'une instruction.
help	Texte d'une instruction système.

SOURCES COMPLÉMENTAIRES D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Anti-Virus 8.0, vous pouvez trouver la réponse via diverses sources d'informations. Parmi elles, vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

Sources d'informations pour une aide autonome	14
Contacteur le service commercial	15
Communication avec le Groupe de rédaction de la documentation technique	15
Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne	15

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez consulter les sources d'informations suivantes sur l'application :

- La page de l'application sur le site de Kaspersky Lab ;
- La page de l'application sur le site du service d'assistance technique (dans la banque de solutions) ;
- Système d'aide électronique ;
- Documentation.

Page du site de Kaspersky Lab

http://www.kaspersky.com/fr/anti-virus_lotus_domino

Sur cette page vous allez retrouver les informations générales sur Kaspersky Anti-Virus, ses possibilités et ses particularités de fonctionnement. Vous pouvez acheter Kaspersky Anti-Virus ou prolonger sa durée d'utilisation dans notre magasin en ligne.

Page sur le site du service d'assistance technique (banque de solutions)

<http://support.kaspersky.com/fr/lotus>

Cette page propose des articles publiés par les experts du service d'assistance technique.

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

Aide électronique

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

Documentation

La documentation qui accompagne Kaspersky Anti-Virus contient la majorité des informations indispensables à l'utilisation de l'application. Elle contient les éléments suivants :

- Le **Guide de l'administrateur** qui contient des informations sur l'utilisation de l'application, sur la configuration des paramètres et sur l'administration de la protection d'un serveur ou d'un groupe de serveurs via le client Lotus, via l'interface Web de l'application ou via la console de serveur Domino.
- Le **Guide de déploiement** permet à l'administrateur de planifier le déploiement de l'application dans 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 sur un serveur ou sur tous les serveurs protégés dans le réseau.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection ou l'achat de Kaspersky Anti-Virus ou sur le renouvellement de la licence, vous pouvez contacter les agents du service vente dans notre bureau de Moscou en composant un des numéros suivants :

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00

Le service est offert en russe et en anglais.

<http://kaspersky.telechargement.fr/>

COMMUNICATION AVEC LE GROUPE DE RÉDACTION DE LA DOCUMENTATION TECHNIQUE

Si vous avez des questions sur la documentation, si vous avez découvert des erreurs ou si vous souhaitez envoyer des commentaires sur nos guides, vous pouvez contacter le groupe de rédaction de la documentation technique.

Envoyez le message avec vos remarques et questions à l'adresse électronique du groupe de rédaction de la documentation technique : docfeedback@kaspersky.com. L'objet du message devra être Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Lotus Domino.

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

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse <http://forum.kaspersky.com/index.php?showforum=107>.

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

KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO

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

Kaspersky Anti-Virus doit être installé sur des serveurs tournant sous des systèmes d'exploitation de la famille Windows ou Linux et il remplit les fonctions suivantes :

- Analyse de tous les messages arrivant sur le serveur Domino du trafic entrant, sortant ou en transit. La recherche de menaces porte sur le texte des messages, les fichiers joints et les objets OLE intégrés. 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 modifiés pendant la réplication. La recherche de menaces porte sur les documents stockés sur le serveur protégé et modifiés suite à la réplication. Les réplifications sortantes ne sont pas analysées. La recherche de menaces porte sur le contenu des champs au format Rich Text, sur les fichiers joints au document et sur les objets OLE insérés dans le document.
- Analyse programmée ou à la demande des bases de données du serveur Domino protégé. La recherche de menaces porte sur le contenu des champs au format Rich Text, sur les fichiers joints au document et sur les objets OLE insérés dans le document.
- Filtrage des objets selon la taille ou le masque de nom lors de l'analyse des messages électroniques, des réplifications et des bases de données. Les objets filtrés sont soumis aux règles de traitement définies par l'administrateur.
- Traitement des objets infectés, potentiellement infectés 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 et des destinataires des messages, ainsi que des administrateurs, sur les objets infectés, potentiellement infectés et non analysés découverts dans les messages ainsi que sur les actions exécutées.
- Notification sur le risque d'épidémie. Kaspersky Anti-Virus consigne les tentatives de diffusion massive d'objets infectés, potentiellement infectés et endommagés dans les messages et prévient les administrateurs.
- Notification des administrateurs sur les objets découverts lors de l'analyse des documents à répliquer et des documents des bases de données ainsi que sur les actions exécutées.
- Conservation dans la base de données Quarantaine des objets infectés et potentiellement infectés. Dans ce cas, les documents et les messages identifiés lors de l'analyse des réplifications et les documents identifiés lors de l'analyse des bases de données sont regroupés par type (courrier/réplication/analyse).
- Conservation des informations sur les objets infectés, potentiellement infectés et non analysés découverts ainsi que sur les actions exécutées dans la base de données Journal des événements et statistiques dans un fichier texte et affichage des informations dans la console du serveur Domino.
- Mise à jour des bases antivirus via Internet, automatiquement ou manuellement. Les sources de mise à jour des bases peuvent être les serveurs HTTP ou FTP de mises à jour de Kaspersky Lab sur Internet, des serveurs HTTP ou FTP contenant l'ensemble des mises à jour ou des répertoires de réseau.

La recherche des menaces et la réparation des objets infectés s'opèrent sur la base des entrées des bases antivirus. Les bases antivirus contiennent les définitions de toutes les menaces connues à ce jour ainsi que les méthodes pour réparer les objets infectés et les définitions des applications potentiellement dangereuses.

Il est primordial de préserver l'actualité des bases car de nouvelles menaces apparaissent chaque jour.

Les bases antivirus sont actualisées toutes les heures sur les serveurs de Kaspersky Lab. Il est conseillé d'actualiser les bases antivirus selon la même fréquence.

- 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 Domino et le navigateur.
- Installation et suppression de l'application via le client Lotus Notes ou via le navigateur Internet.

DANS CETTE SECTION

Nouveautés	17
Distribution	18
Service pour les utilisateurs enregistrés	18
Configurations logicielle et matérielle	18

NOUVEAUTÉS

Voici les principales différences entre Kaspersky Anti-Virus 8.0 for Lotus Domino et la version antérieure :

- Perfectionnement des méthodes de découverte de menaces grâce à l'utilisation d'un nouveau moteur antivirus.
- Augmentation du nombre de plateformes prises en charge.
- Interface intuitive.
- Possibilité d'administrer l'application via le client Lotus Notes ou via le navigateur Internet.
- Augmentation du nombre d'instructions disponibles pour l'administration de Kaspersky Anti-Virus via la console du serveur Domino.
- Possibilité d'installer l'application via le client Lotus Notes ou via le navigateur Internet.
- Possibilité de réaliser une configuration groupée des paramètres et l'administration centralisée de l'application installée sur plusieurs serveurs grâce aux profils.
- Prise en charge d'un schéma distribué d'administration des paramètres de la sécurité des serveurs protégés.
- Prise en charge de la tenue distribuée du journal des événements et des statistiques du fonctionnement de l'application sur tous les serveurs protégés.
- Introduction de l'administration des privilèges des utilisateurs au niveau des bases de données et au niveau de documents distincts.

- Prise en charge de l'analyse des objets dans la mémoire vive du serveur sans enregistrement sur le disque dur.
- Possibilité d'ajouter à l'objet du message des informations sur son analyse par Kaspersky Anti-Virus. Les informations sont organisées selon le modèle créé par l'administrateur.

DISTRIBUTION

Vous pouvez acheter Kaspersky Anti-Virus chez nos partenaires (version en boîte) ou en ligne (par exemple, <http://www.kaspersky.fr>, rubrique **Boutique en ligne**).

Si vous achetez Kaspersky Anti-Virus en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce guide. Le fichier de licence vous sera envoyé par courrier électronique après le paiement.

SERVICE POUR LES UTILISATEURS ENREGISTRÉS

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

Au moment d'obtenir la licence, vous devenez un utilisateur enregistré et vous pouvez utiliser les services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases antivirus et offre des nouvelles versions de cette application ;
- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;
- Notifications sur la diffusion de nouveaux logiciels de Kaspersky Lab ou sur l'émergence de nouveaux virus. Ce service est offert aux utilisateurs qui se sont abonnés au bulletin d'informations de Kaspersky Lab sur le site du service d'Assistance technique (<http://support.kaspersky.com/fr/subscribe>).

Les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, des applications d'éditeurs tiers ou aux différentes technologies ne seront pas traitées.

CONFIGURATIONS LOGICIELLE ET MATÉRIELLE

Pour garantir le fonctionnement normal de Kaspersky Anti-Virus, l'ordinateur doit remplir les conditions minimales suivantes.

Configuration matérielle :

- Intel Pentium 32 bits / 64 bits ou supérieur (ou analogue).
- 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 matérielle:

Systèmes d'exploitation compatibles :

Plateformes 32 bits :

- Microsoft Windows 2000 Server (Service Pack 4 et suivant).
- Microsoft Windows 2000 Advanced Server (Service Pack 4 et suivant).
- Microsoft Windows Server 2003 Standard Edition (Service Pack 2).
- Microsoft Windows Server 2003 Enterprise Edition (Service Pack 2).
- Novell SuSE Linux Enterprise Server 10 (Service Pack 2).
- Red Hat Enterprise Linux 5 (Service Pack 3).

Plateformes 64 bits :

- Microsoft Windows Server 2003 x64 Enterprise Edition (Service Pack 2).
- Novell SuSE Linux Enterprise Server 10 (Service Pack 2).
- Red Hat Enterprise Linux 5 (Service Pack 3).

Serveurs Lotus Notes/Domino compatibles :

- Lotus Notes/Domino version 6.5.
- Lotus Notes/Domino version 7.0.
- Lotus Notes/Domino version 8.0.
- Lotus Notes/Domino version 8.5.

Navigateurs compatibles :

- Windows Internet Explorer 7.
- Windows Internet Explorer 8.
- Mozilla Firefox 3.6.
- Google Chrome.

ARCHITECTURE DE L'APPLICATION

Kaspersky Anti-Virus contient les modules suivants :

- **Module d'administration** : il permet à Kaspersky Anti-Virus de remplir les fonctions suivantes :
 - Administration de l'application : initialise l'analyse du courrier et des réplifications, lance l'analyse des bases de données et la mise jour programmée des bases antivirus.
 - Administration des paramètres de fonctionnement de l'application : récupère et applique les nouvelles valeurs des paramètres.
 - Enregistrement et analyse des données statistiques : 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 envoi des notifications aux administrateurs.
 - Notification : envoi des notifications électroniques sur les objets infectés, potentiellement infectés et endommagés découverts pendant l'analyse.
 - Notification sur les épidémies : suivi du nombre d'objets infectés, potentiellement infectés et endommagés découverts lors de l'analyse du courrier et notification sur le nombre de messages contenant la même menace et alerte l'administrateur lorsque le nombre d'objets découverts au cours d'une période déterminée dépasse la valeur définie.
 - Administration des licences : activation des licences, analyse des informations de la licence, installation et suppression du fichier de licence.
- **Module d'analyse du courrier et des réplifications** : réalise l'analyse antivirus des messages électroniques et des réplifications.
- **Module d'analyse des bases de données** : réalise l'analyse antivirus des bases de données du serveur domino.

Tous les modules sont chargés automatiquement au démarrage du serveur Domino. Les informations relatives au fonctionnement du module sont consignées dans la base de données Journal des événements et statistiques, sont consignées dans le fichier du journal de Kaspersky Anti-Virus et affichées dans la console du serveur Domino.

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

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. rubrique " Administration des paramètres de Kaspersky Anti-Virus " à la page [24](#)) ;
- Base de données Quarantaine (kavquarantine.nsf) : elle sert à conserver les objets placés en quarantaine et à les manipuler (cf. page [88](#)) ;
- Base de données Journal des événements et statistiques (kaveventslog.nsf) : elle sert à conserver 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 l'exécution sur ceux-ci des actions (cf. rubrique " Journal des événements et statistiques " à la page [95](#)) ;
- 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. rubrique " Interface de l'application " à la page [36](#)).

DANS CETTE SECTION

Schéma de la protection antivirus du serveur.....21

Administration des paramètres de Kaspersky Anti-Virus.....24

Administration des paramètres du fichier de configuration notes.ini.....26

Administration des privilèges.....28

SCHÉMA DE LA PROTECTION ANTIVIRUS DU SERVEUR

Kaspersky Anti-Virus assure la protection des réplifications et analyse les bases de données conservées sur le serveur. La protection du serveur est assurée par les composants suivants : protection du courrier, protection des réplifications et analyse des bases de données.

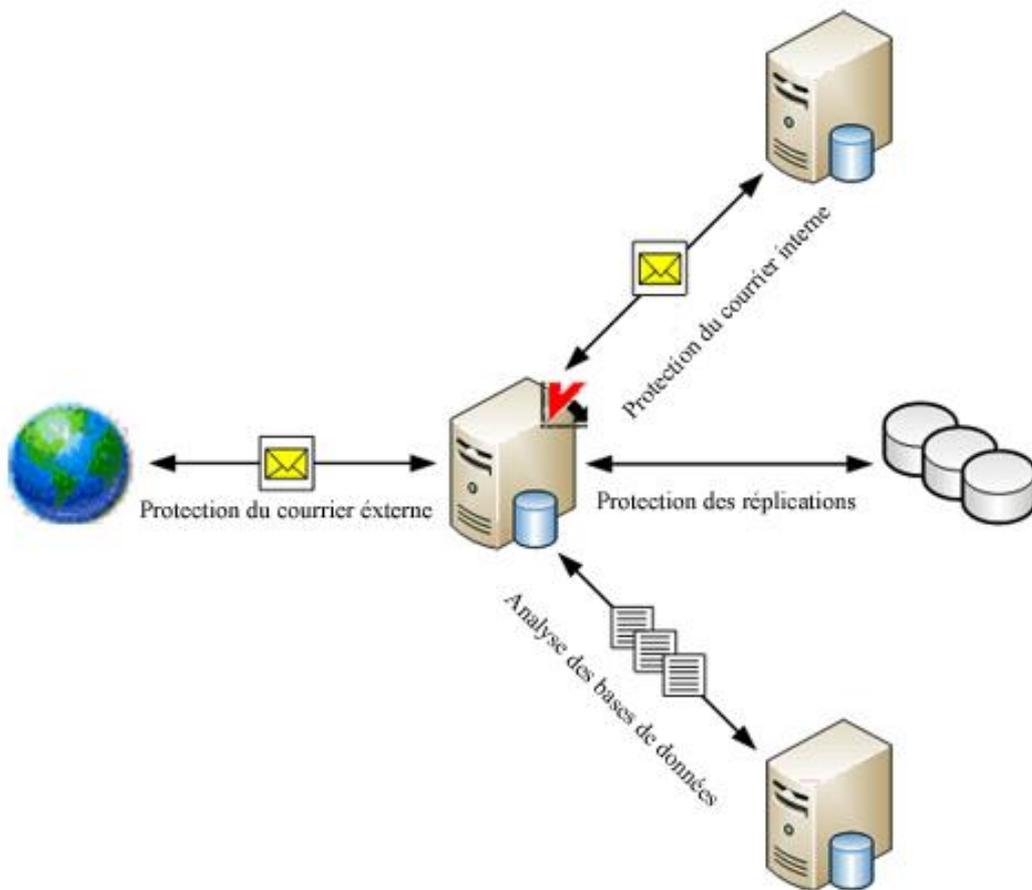


Illustration 1 : Schéma de la protection antivirus du serveur Domino

DANS CETTE SECTION

Schéma de fonctionnement de l'application	22
Algorithme de la recherche d'éventuelles menaces dans les objets.....	23
Algorithme de filtrage des pièces jointes	23
Traitement des objets et actions exécutées sur ceux-ci	24

SCHÉMA DE FONCTIONNEMENT DE L'APPLICATION

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

1. Le **Module d'administration** reçoit du serveur Domino des informations sur le message électronique qui arrive dans la base de données mail.box sur le serveur protégé ou sur la tentative de répliquions sur le serveur protégé. Le **Module d'administration** transmet le message ou le document modifié suite à la répliquion au **Module d'analyse du courrier et des répliquions**.
2. Le **Module d'analyse du courrier et des répliquions** analyse le message/le document et le traite selon les paramètres de la protection du courrier ou des répliquions. Les actions suivantes sont alors exécutées :
 - 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, les pièces jointes et les objets OLE sont séparés.
 - Le filtrage des objets joints (cf. la rubrique " Algorithme de filtrage des pièces jointes " à la page [23](#)) selon la taille et (ou) le nom est réalisé.
 - L'analyse antivirus des objets (cf. la rubrique " Algorithme de la recherche d'éventuelles menaces dans les objets " à la page [23](#)) est exécutée.
 - Les objets sains sont ignorés sans modifications tandis que les autres sont traités conformément aux paramètres de la protection (cf. rubrique " Traitement des objets et actions exécutées sur ceux-ci " à la page [24](#)). Avant de passer au traitement, il est possible de conserver une copie de l'objet dans la base de données Quarantaine.
 - Les messages traités sont transmis au système de messagerie du serveur Domino pour envoi. Les documents traités sont conservés dans les bases de données.
3. Le **module d'administration**, conformément aux paramètres de notification sur les épidémies, additionne le nombre d'objets infectés, potentiellement infectés et endommagés découverts pendant l'analyse du courrier ainsi que le nombre d'objets contenant la même menace (cf. la rubrique " Notifications sur les épidémies " à la page [66](#)).
4. Conformément à la programmation de l'analyse des bases ou suite à l'instruction manuelle d'exécution, le **Module d'administration** transmet au **Module d'analyse** des bases de données l'instruction pour lancer l'analyse. Le **module d'analyse des bases de données** établit la liste des documents à vérifier conformément aux paramètres d'analyse, puis analyse les documents conformément à cette liste. L'algorithme d'analyse d'un document correspond en tout point à l'algorithme d'analyse d'un document par le **module d'analyse du courrier et des répliquions**.

ALGORITHME DE LA RECHERCHE D'ÉVENTUELLES MENACES DANS LES OBJETS

Kaspersky Anti-Virus analyse l'objet soumis à l'analyse antivirus 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 contiennent la description de tous les programmes malveillants, jokewares, riskwares ou programmes qui ne sont pas des riskwares mais qui peuvent contribuer à leur développement connus au moment de la création des bases ainsi que les outils de neutralisation.

L'analyse des objets est réalisée via une analyse incrémentielle : les fichiers sont à nouveau analysés uniquement après modification, c à-d. que si la date de la dernière modification des fichiers est antérieure à la date de la dernière analyse, le fichier ne sera pas analysé. Pour désactiver l'analyse incrémentielle, définissez la variable KAVNonIncrementalScan=1. Cette variable est absente par défaut.

Suite à l'analyse, l'objet reçoit un des états suivants :

- *sain* : l'objet ne contient pas de menace ;
 - *irréparable* : l'objet contient une menace qui ne peut pas être neutralisée à l'aide de la version actuelle des bases antivirus ; ces objets ne peuvent pas être réparés ;
 - *réparable* : l'objet contient une menace qui peut être neutralisée à l'aide de la version actuelle des bases antivirus ; après la réparation, l'objet sera considéré comme sain ;
 - *non analysé* : Kaspersky Anti-Virus n'a pas pu analyser l'objet ; il se peut qu'il s'agisse d'une archive protégée par un mot de passe ou compressée à l'aide d'un algorithme inconnu ou qu'une erreur se soit produite pendant l'analyse de l'objet, ou que le temps prévu pour l'analyse soit écoulé.
2. L'objet considéré comme sain à l'issue de l'analyse à l'aide des bases antivirus est analysé à l'aide de l'analyseur heuristique. Dans ce contexte, Kaspersky Anti-Virus emploie des mécanismes spéciaux pour analyser l'activité de l'objet dans le système. Si cette activité est caractéristique des objets malveillants, l'objet reçoit l'état *potentiellement infecté* : cela signifie que 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.

ALGORITHME DE FILTRAGE DES PIÈCES JOINTES

Kaspersky Anti-Virus filtre les objets joints aux messages et aux documents. Si l'objet satisfait les conditions du filtre, il reçoit l'état défini dans les paramètres du filtre. La suite de l'analyse antivirus de l'objet n'a pas lieu. L'objet est traité conformément à l'état attribué par le filtre : l'objet est soumis aux actions définies pour les objets de cet état dans les paramètres de la protection du courrier, de la protection des répliqués et de l'analyse des bases de données (cf. rubrique " Traitement des objets et actions exécutées sur ceux-ci " à la page [24](#)).

L'application propose les types de filtrage 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 maximum 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 satisfait le 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 de filtrage, l'objet sera soumis à l'analyse antivirus.

Si les deux types de filtrage des pièces jointes sont définis dans les paramètres de la protection, Kaspersky Anti-Virus analysera 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 selon la taille, Kaspersky Anti-Virus ne vérifiera pas le nom de l'objet.

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

- sain ;
- irréparable ;
- non analysé ;
- potentiellement infecté.

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

TRAITEMENT DES OBJETS ET ACTIONS EXÉCUTÉES SUR CEUX-CI

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus (cf. rubrique " Algorithme de la recherche d'éventuelles menaces dans les objets " à la page [23](#)) et suite au filtrage des pièces jointes (cf. rubrique " Algorithme de filtrage des pièces jointes " à la page [23](#)). Les objets sains sont transmis sans aucune modification aux bases de données du serveur Domino (protection des répliquions et analyse des bases de données) ou au système de messagerie du serveur Domino (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 sur 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 possible uniquement pour les objets qui peuvent être réparés.

Peu importe la configuration des paramètres, la réparation des objet OLE s'effectue uniquement à l'aide d'une suppression.

- **Ignorer.** Kaspersky Anti-Virus transmet l'objet 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 séparément dans les paramètres de la protection du courrier, de la protection des répliquions 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 (cf. rubrique " Notifications " à la page [106](#)).

ADMINISTRATION DES PARAMÈTRES DE KASPERSKY ANTI-VIRUS

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

Un *profil* définit les paramètres généraux de l'application pour un groupe de serveurs repris dans ce profil. Le recours aux profils permet de réaliser une gestion centralisée des paramètres de Kaspersky Anti-Virus.

Le profil peut contenir plusieurs serveurs ou un seul. En cas de déploiement isolé de Kaspersky Anti-Virus, le profil contient uniquement un serveur (cf. Guide de déploiement 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. rubrique " Définition de valeurs individuelles pour les paramètres du serveur " à la page [112](#)). De plus, il est possible de redéfinir certains paramètres du profil dans les paramètres du serveur. Cette possibilité permet de définir pour un serveur distinct des paramètres qui correspondent au rôle du serveur dans le système de la protection antivirus et différents 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. rubrique " Création et suppression de profils " à la page [109](#)). Le serveur sur lequel Kaspersky Anti-Virus est installé peut être déplacé d'un profil vers un autre (cf. rubrique " Déplacement du serveur vers un autre profil " à la page [112](#)).

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.

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. rubrique " Définition de valeurs individuelles pour les paramètres du serveur " à la page [112](#)). Ainsi, les paramètres du serveur peuvent intervenir dans la configuration du modèle de mise à jour centralisé des bases antivirus (cf. rubrique " Schémas de mise à jour " à la page [51](#)).

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.

Dans le contexte d'un déploiement distribué de Kaspersky Anti-Virus (cf. Guide de déploiement de Kaspersky Anti-Virus 8.0 for Lotus Domino), la base de données kavcontrolcenter.nsf contient des informations sur les paramètres de fonctionnement de Kaspersky Anti-Virus sur chacun des serveurs où l'application est installée. La base de données est créée pendant l'installation sur 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 d'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 d'où 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 un des serveurs, les informations relatives à ce serveur sont supprimées du profil dans la base de données Centre d'administration.

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

Pour configurer les paramètres de Kaspersky Anti-Virus et pour administrer son fonctionnement, il faut 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 d'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité**, **Administrateurs du centre d'administration** **Administrateur avec des privilèges restreints**. Avant d'ouvrir la base de données, assurez-vous que le compte utilisateur possède les autorisations 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. rubrique " Interface de l'application " à la page [36](#)).

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. Il peut y avoir un certain délai 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 faut tenir compte de la topologie des réplifications.

Si vous utilisez Kaspersky Anti-Virus via le client de Lotus Notes, les modifications des paramètres peuvent 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 la connexion a été réalisée (cf. rubrique " Exploitation de la possibilité de modification directe des paramètres du serveur " à la page [114](#)). Dans ce cas, les nouvelles valeurs des paramètres du serveur sont appliquées bien plus vite. En cas d'utilisation via le navigateur Internet, la possibilité décrite ci-dessus n'est pas prise en charge et les modifications des paramètres du serveur sont toujours introduites dans la réplique ouverte.

Si la case **Modifier le document sur le serveur protégé** du groupe **Administration de la configuration** du document serveur sous l'onglet **Paramètres généraux** est cochée, alors le document est ouvert depuis une réplique de la base de données située sur le serveur correspondant à ce document de serveur. Sur un client de la version 8 ou plus, le document est ouvert d'un clic sur le document du serveur dans le panneau de navigation. Sur les clients plus anciens, il faut double-cliquer. Si vous cliquez une seule fois sur un document dans une version plus ancienne du client, le document s'ouvre depuis une réplique située sur le serveur actif.

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 réplifications. 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 de nouveaux paramètres du profil, les paramètres du serveur peuvent être redéfinis automatiquement.

ADMINISTRATION DES PARAMÈTRES DU FICHER DE CONFIGURATION NOTES.INI

L'administration des paramètres de Kaspersky Anti-Virus peut être réalisée via l'interface ou à l'aide de modifications dans le fichier de configuration notes.ini.

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

1. Ouvrez le fichier notes.ini contenant les paramètres du serveur Domino.
2. Modifiez les paramètres et enregistrez les modifications.
3. Relancez le serveur 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 ont priorité sur les paramètres de l'interface.

Tableau 2. Liste des paramètres modifiables

PARAMÈTRES	VALEUR	DESCRIPTION
EXTMGR_ADDINS	Chemin d'accès à kavmailhook	L'intercepteur fonctionne.
	0 / absence de valeur de la variable	L'intercepteur ne fonctionne pas. ATTENTION : l'absence de paramètre est identique à la suppression de Kaspersky Anti-Virus sur le serveur.
KAVDefaultLogLevel	0	Standard.
	1	Etendu.
	2	Débogage.
KAVCustomUpdUrlOnly	1	Le serveur sera mis à jour uniquement depuis la source de mise à jour que vous aurez indiquée.
	2	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 le serveur de mises à jour de Kaspersky Lab.
KAVDefaultLogFileName	server est la valeur par défaut	Nom du fichier des journaux Vous pouvez attribuer n'importe quelle valeur à ce paramètre. Le fichier des journaux créé portera le nom indiqué dans cette variable : Le fichier sera enregistré dans le répertoire des journaux " kavcommon/logs/ ". Par défaut, le nom du fichier sera créé selon le principe suivant : <Nom du fichier>.log_N, où N est le numéro de séquence du log. Si vous attribuez à ce paramètre la valeur monfichier, les événements seront conservés dans le fichier monfichier.log_N.
KAVLogFileSize	2 000 Ko	Taille d'un fichier de journal en kilooctets. Un écart de 5 % par rapport au paramètre défini est admis pour optimiser la vitesse.
KAVLogFilesNumber	5	Nombre de fichiers de journal.
KAVArchDepthLevel	32	Niveau d'imbrication des archives.
	0 / absence de paramètres	Le niveau d'imbrication n'est pas défini.
KAVNonIncrementalScan	0 / absence de variable	L'analyse incrémentielle est activée.
	1	L'analyse incrémentielle est désactivée.

ADMINISTRATION DES PRIVILÈGES

L'administration des privilèges des utilisateurs de l'application s'opère au niveau de la LCA des bases de données de Kaspersky Anti-Virus et au niveau des documents distincts (paramètres du profil et paramètres du serveur). Les privilèges au niveau de la LCA sont octroyés à l'aide du mécanisme des groupes fonctionnels (cf. rubrique " Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus. " à la page [28](#)). Les privilèges au niveau des documents sont octroyés à l'aide des rôles fonctionnels (cf. rubrique " Administration des privilèges au niveau des paramètres du profil/serveur " à la page [31](#)).

DANS CETTE SECTION

Administration des privilèges au niveau de la LCA des bases de données de Kaspersky Anti-Virus.....[28](#)

Administration des privilèges au niveau des paramètres du profil/serveur[31](#)

ADMINISTRATION DES PRIVILÈGES AU NIVEAU DE LA LCA DES BASES DE DONNÉES 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 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 (cf. Guide de déploiement). 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).

PRIVILÈGES 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 DONNÉES CENTRE D'ADMINISTRATION	BASE DE DONNÉES JOURNAL DES ÉVÉNEMENTS ET STATISTIQUES	BASE DE DONNÉES QUARANTAINE	BASE DE DONNÉES AIDE
ADMINISTRATEURS DE LA SÉCURITÉ	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. 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. 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 PRIVILÈGES 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 de la base 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. rubrique " Administration des privilèges au niveau des paramètres du profil/du serveur " à la page [31](#)).

Les utilisateurs des trois groupes fonctionnels peuvent consulter les entrées des bases Quarantaine, Journal des événements et statistiques et Aide.

OCTROI DE PRIVILÈGES DES GROUPES FONCTIONNELS AUX UTILISATEURS

Pendant l'installation de Kaspersky Anti-Virus, l'administrateur peut inclure dans chacun des trois groupes fonctionnels aussi bien des utilisateurs individuels de Domino que des groupes d'utilisateurs.

Pour simplifier la procédure d'octroi des privilèges, il est conseillé de ne pas inclure des utilisateurs individuels dans les groupes fonctionnels, mais bien les groupes composés dans le carnet d'adresses du serveur Domino (cf. Guide de déploiement). 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. rubrique " Privilèges des groupes fonctionnels " à la page [29](#)). Plus tard, l'administrateur du serveur 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 faut 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 faut 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 à l'utilisateur les privilèges d'un groupe fonctionnel, il faut procéder comme suit :*

1. Créer dans le carnet d'adresses du serveur Domino un groupe portant un nom unique, par exemple ControlCenterAdmins.
2. Ajouter l'utilisateur qui va recevoir les privilèges de tel ou tel groupe fonctionnel, par exemple du groupe **Administrateurs du centre d'administration**, au groupe ControlCenterAdmins.
3. Ouvrir une session dans le système sous le compte de l'utilisateur possédant les privilèges du groupe fonctionnel **Administrateur de la sécurité**.
4. Ajouter 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 définir pour le groupe ControlCenterAdmins les privilèges qui correspondent aux privilèges du groupe fonctionnel **Administrateur du Centre d'administration** (cf. rubrique " Privilèges des groupes fonctionnels " à la page [29](#)).

ADMINISTRATION DES PRIVILÈGES AU NIVEAU DES PARAMÈTRES 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 :

- *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.
- *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. rubrique " Désignation de l'administrateur de serveur " à la page [111](#)) et chaque profil séparément (cf. rubrique " Désignation de l'administrateur de profil " à la page [111](#)).

Seul un utilisateur possédant les privilèges d'un des trois groupes fonctionnels peut être désigné comme administrateur de profil ou administrateur de serveur (cf. rubrique " Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus. " à la page [28](#)).

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 faut 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.

ADMINISTRATION DES LICENCES

Il est primordial de comprendre les notions suivantes dans le cadre de l'octroi des licences pour les applications de Kaspersky Lab :

- Le contrat de licence ;
- La licence ;
- Le fichier de licence.

Ces trois notions sont étroitement liées et forment un modèle unique de licence.

Examinons chacune d'entre elles en détail.

DANS CETTE SECTION

Présentation du contrat de licence	32
Présentation des licences de Kaspersky Anti-Virus	33
Présentation des fichiers de licence de Kaspersky Anti-Virus	33
Installation du fichier de licence.....	34

PRÉSENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un contrat entre une personne physique ou juridique possédant une copie de Kaspersky Anti-Virus et Kaspersky Lab, Ltd. Ce contrat accompagne chaque application de Kaspersky Lab. Il détaille les droits et les limites d'utilisation de Kaspersky Anti-Virus.

Ce guide reprend le texte du contrat de licence (cf. rubrique " Texte du contrat de licence " à la page [3](#)).

Conformément au contrat de licence, en achetant et en installant l'application de Kaspersky Lab, vous obtenez le droit de posséder pour une durée indéterminée une copie.

Kaspersky Lab est également ravi de vous offrir des services complémentaires :

- assistance technique ;
- mise à jour des bases de Kaspersky Anti-Virus ;
- mise à jour des modules logiciels de Kaspersky Anti-Virus.

Pour en profiter, vous devez acheter et activer une licence.

PRÉSENTATION DES LICENCES DE KASPERSKY ANTI-VIRUS

La *licence* est le droit d'utilisation de Kaspersky Anti-Virus et des services complémentaires que vous confère Kaspersky Lab ou ses partenaires.

Chaque licence est caractérisée par sa durée de validité et son type.

La *durée de validité de la licence* est la période au cours de laquelle vous pouvez bénéficier des services complémentaires. Le type de services dépend du type de licence.

Il existe différents types de licence :

Évaluation : licence gratuite à durée de validité limitée. Cette licence permet de découvrir Kaspersky Anti-Virus. Elle est installée avec la version d'évaluation de l'application et sa durée de validité est courte. Tant que vous utilisez une licence d'évaluation, vous ne pouvez pas contacter le service d'assistance technique et une fois la durée de validité expirée, toutes les fonctions de Kaspersky Anti-Virus sont désactivées.

Commerciale : licence payante dont la durée de validité est d'au moins un an. L'utilisateur obtient cette licence à l'achat de l'application. Une fois la durée de validité de la licence commerciale écoulée, Kaspersky Anti-Virus continue à fonctionner mais les services complémentaires ne sont plus accessibles.

Pour pouvoir continuer à utiliser l'application et les services complémentaires, il faut acheter une licence commerciale et l'activer.

L'activation de la licence s'opère en installant le fichier de licence associé à la licence.

PRÉSENTATION DES FICHIERS DE LICENCE DE KASPERSKY ANTI-VIRUS

Le *fichier de licence* est le moyen technique qui permet d'activer la licence associée.

Le fichier de licence est livré avec le fichier d'installation de l'application si vous achetez l'application chez un revendeur ou vous le recevez par courrier électronique en cas d'achat en ligne.

Le fichier de licence reprend les informations suivantes :

- Durée de validité de la licence.
- Type de licence (évaluation ou commerciale).
- Restrictions imposées par la licence (par exemple, le nombre d'ordinateurs couverts par la licence ou le volume de trafic de messagerie protégé).
- Coordonnées du Service d'assistance technique.
- Durée de validité du fichier de licence.

La *durée de validité du fichier de licence* désigne, comme son nom l'indique, la durée de validité à partir de sa date de diffusion. Il s'agit de la période à l'issue de laquelle le fichier n'est plus valide et n'est plus en mesure d'activer la licence associée.

Prenons un exemple pour montrer la relation entre la durée de validité du fichier de licence et la durée de validité de la licence.

Exemple :

Durée de validité de la licence : 300 jours

Date d'édition du fichier de licence : 11/01/2010

Durée de validité du fichier de licence : 300 jours

Date d'installation du fichier de licence (activation de la licence) : 20/01/2010, soit 9 jours après sa diffusion.

Résultats :

Durée calculée de la validité de la licence : 300 jours - 9 jours = 291 jours.

INSTALLATION DU FICHIER DE LICENCE

L'installation du fichier de licence doit avoir lieu sur chaque serveur séparément. Vous pouvez installer deux fichiers de licence : un fichier de licence actif et un fichier de licence de réserve. Le fichier de licence actif entre en vigueur dès son installation. L'application ne peut pas compter plus d'une licence active. Le fichier de licence de réserve est utilisé automatiquement à l'échéance de la validité du fichier actif. Les fichiers de licence peuvent être installés lors de l'installation de Kaspersky Anti-Virus.

Avant d'installer le fichier de licence via l'interface de la console du serveur Domino, assurez-vous que le fichier de licence est bien accessible via le système de fichiers du serveur sur lequel il est installé. En cas d'installation du fichier de licence via le client Lotus Notes ou via le navigateur Internet, assurez-vous qu'il est accessible via le système de fichiers du poste client où la base de données Centre d'administration a été ouverte.

➔ Pour installer le fichier de licence, procédez comme suit :

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous voulez installer le fichier de licence.
3. Dans la zone d'administration, choisissez l'onglet **Licence** (cf. ill. ci-après).
4. Cliquez sur le bouton **Ajouter le fichier de licence**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de licence portant l'extension key, puis cliquez sur le bouton **Ouvrir**.

Le fichier de licence indiqué sera installé sur le serveur (cf. ill. ci-après).

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

- **Fonctionnalité.** Les restrictions suivantes sont prévues au niveau de la fonctionnalité :
 - **Complet** : la licence est installée.
 - **Uniquement l'administration** : la licence 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 licence 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 de fin de validité.** Date de fin de validité de la licence.
- **Jours restant.** Durée pendant laquelle vous bénéficierez des services complémentaires.
- **Numéro de la licence.** Numéro de série de la licence.
- **Informations sur le détenteur.** Informations sur le détenteur de la licence : organisation, nom du détenteur, pays, courrier électronique, etc.

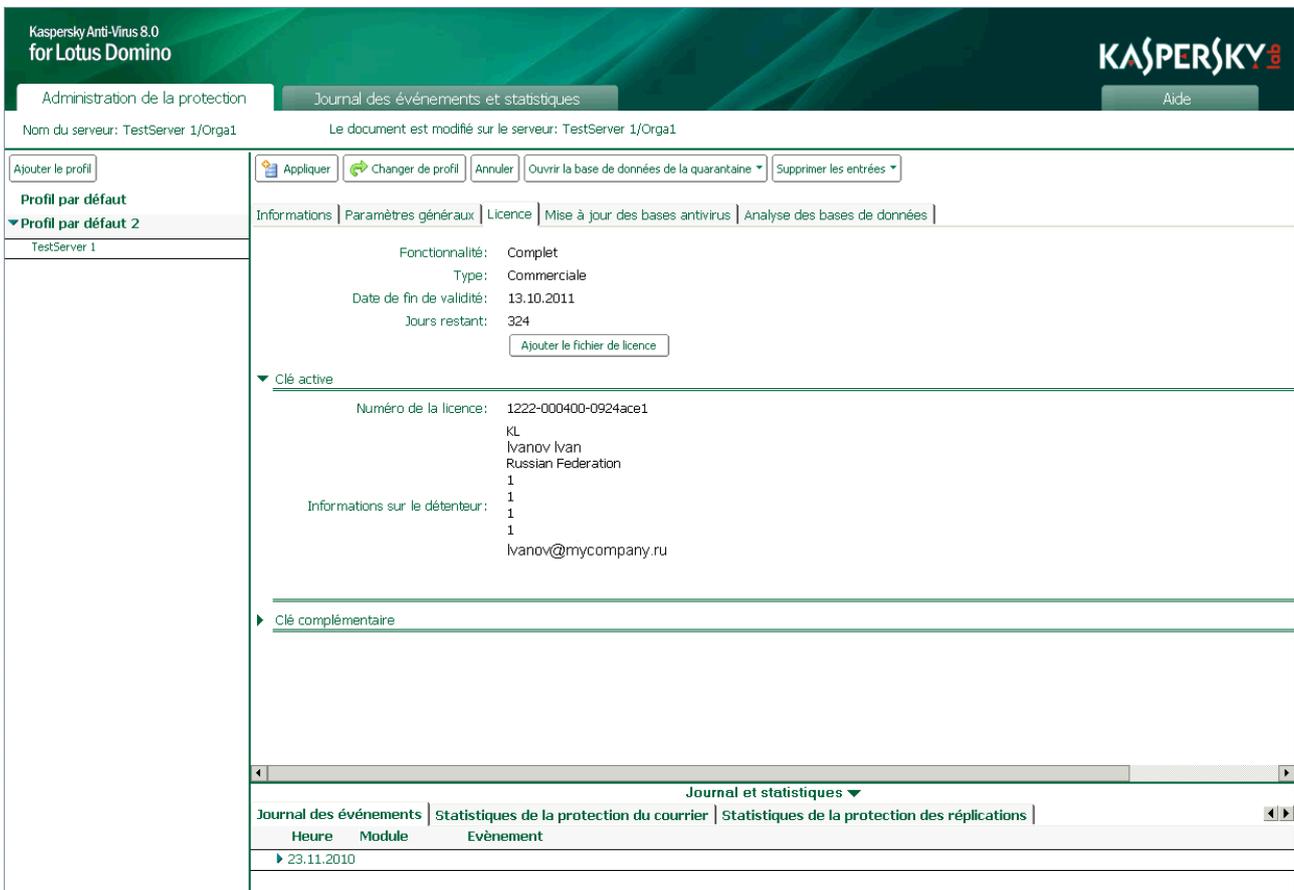


Illustration 2: Consultation des informations relatives à la licence

La suppression du fichier de licence actif ou de réserve est uniquement possible via la ligne de commande (cf. rubrique " Utilisation via la console du serveur " à la page [119](#)).

INTERFACE DE L'APPLICATION

Cette rubrique décrit les principaux éléments de l'interface de Kaspersky Anti-Virus.

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. La fenêtre de la base de données Centre d'administration permet également d'utiliser les bases de données Quarantaine, Journal des événements et statistiques et Aide.

La base de données est accessible via le client Lotus Notes ou via le navigateur Internet. L'interface Web permet de gérer l'application depuis des ordinateurs qui ne seraient pas équipés du client Lotus Notes.

Il existe également une série d'instructions pour l'administration de Kaspersky Anti-Virus via la console du serveur Domino (cf. rubrique " Utilisation via la console du serveur " à la page [119](#)).

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 d'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité** , **Administrateurs du centre d'administration** **Administrateur avec des privilèges restreints**. Avant d'ouvrir la base de données, assurez-vous que le compte utilisateur possède les autorisations 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, utilisez une des méthodes suivantes :*

- Via le client Lotus Notes, ouvrez la base de données kavcontrolcenter.nsf sur un des serveurs avec Kaspersky Anti-Virus installé ;
- Ouvrez le navigateur Internet et saisissez l'adresse :

```
http://<nom_du_serveur>/<chemin_d'accès_au_fichier_kavcontrolcenter.nsf>?OpenDatabase
```

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 par rapport au répertoire des données du serveur.

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

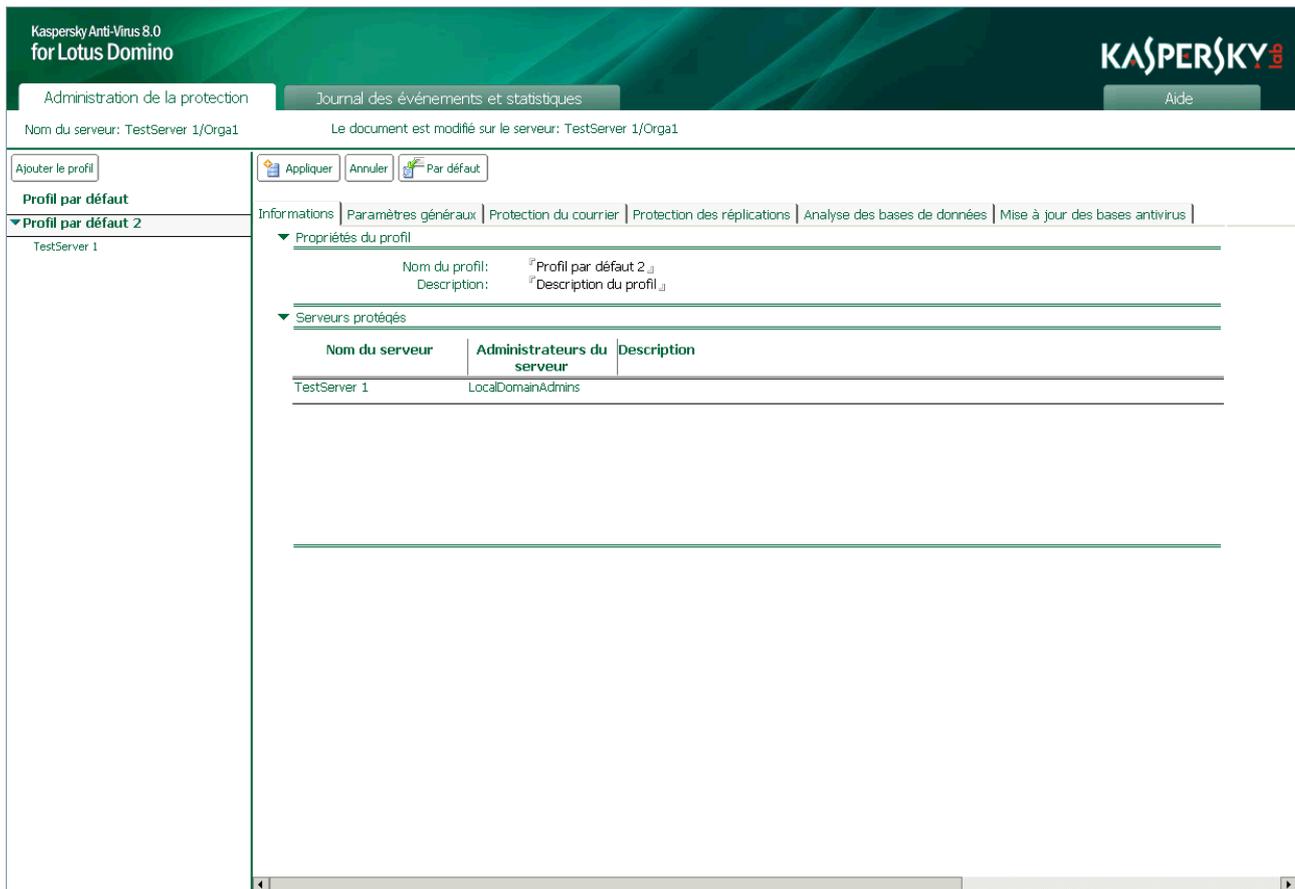


Illustration 3 : Fenêtre de la base de données Centre d'administration

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 la base de données. 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.

DANS CETTE SECTION

Structure de la fenêtre de la base de données Centre d'administration	38
Onglet Administration de la protection.....	39
Onglet Journal des événements et statistiques	42
Onglet Aide.....	43

STRUCTURE DE LA FENÊTRE DE LA BASE DE DONNÉES 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 (cf. rubrique " Exploitation de la possibilité de modification directe des paramètres du serveur " à la page [114](#)).

- *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 ;
 - Table des matières du système d'aide de Kaspersky Anti-Virus.

- **Zone d'administration** et **zone de consultation** : situées dans la partie droite de la fenêtre, ces zones permettent de manipuler les paramètres des profils/des serveurs, les entrées des bases données de Kaspersky Anti-Virus et de consulter l'aide de Kaspersky Anti-Virus.

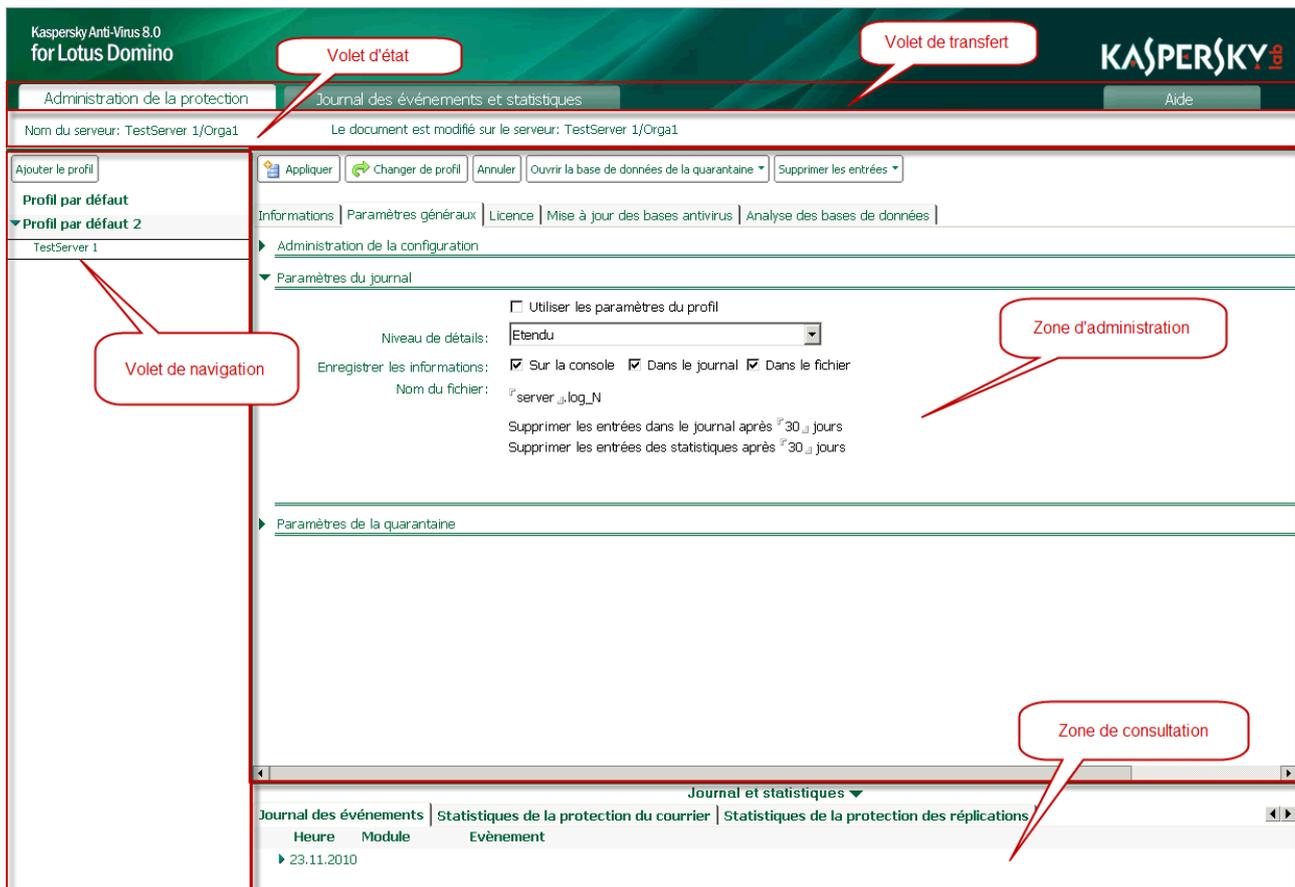


Illustration 4 : Structure de la fenêtre de la base de données Centre d'administration

Le contenu du volet de navigation, de la zone d'administration et de la zone 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** permet de travailler avec la base de données Centre d'administration : configuration des paramètres de fonctionnement de Kaspersky Anti-Virus sur les serveurs protégés et configuration des paramètres de la protection antivirus (protection du courrier, protection des réplifications, analyse des bases de données et mise à jour des bases antivirus, etc.).

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

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

Le bouton **Ajouter le profil**, prévu pour la création d'un profil (cf. rubrique " Création et suppression de profils " à la page 109) 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 la zone 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 productivité de l'application (cf. rubrique " Productivité " à la page [86](#)) et les paramètres du Journal des événements et statistiques pour les serveurs appartenant au profil (cf. rubrique " Configuration des paramètres du journal des événements " à la page [96](#)).
- **Protection du courrier.** L'onglet permet de configurer les paramètres de la protection du courrier pour les serveurs qui sont repris dans le profil (cf. page [57](#)).
- **Protection des répliquions.** L'onglet permet de configurer la protection des répliquions pour les serveurs qui figurent dans le profil (cf. rubrique " Protection des répliquions " à la page [69](#)).
- **Analyse des bases de données.** L'onglet permet de configurer les paramètres de l'analyse des bases de données pour les serveurs qui sont repris dans le profil (cf. page [76](#)).
- **Mise à jour des bases antivirus.** L'onglet permet de configurer les paramètres de la mise à jour pour les serveurs qui figurent dans le profil (cf. rubrique " Sélection de la source des mises à jour " à la page [53](#)).

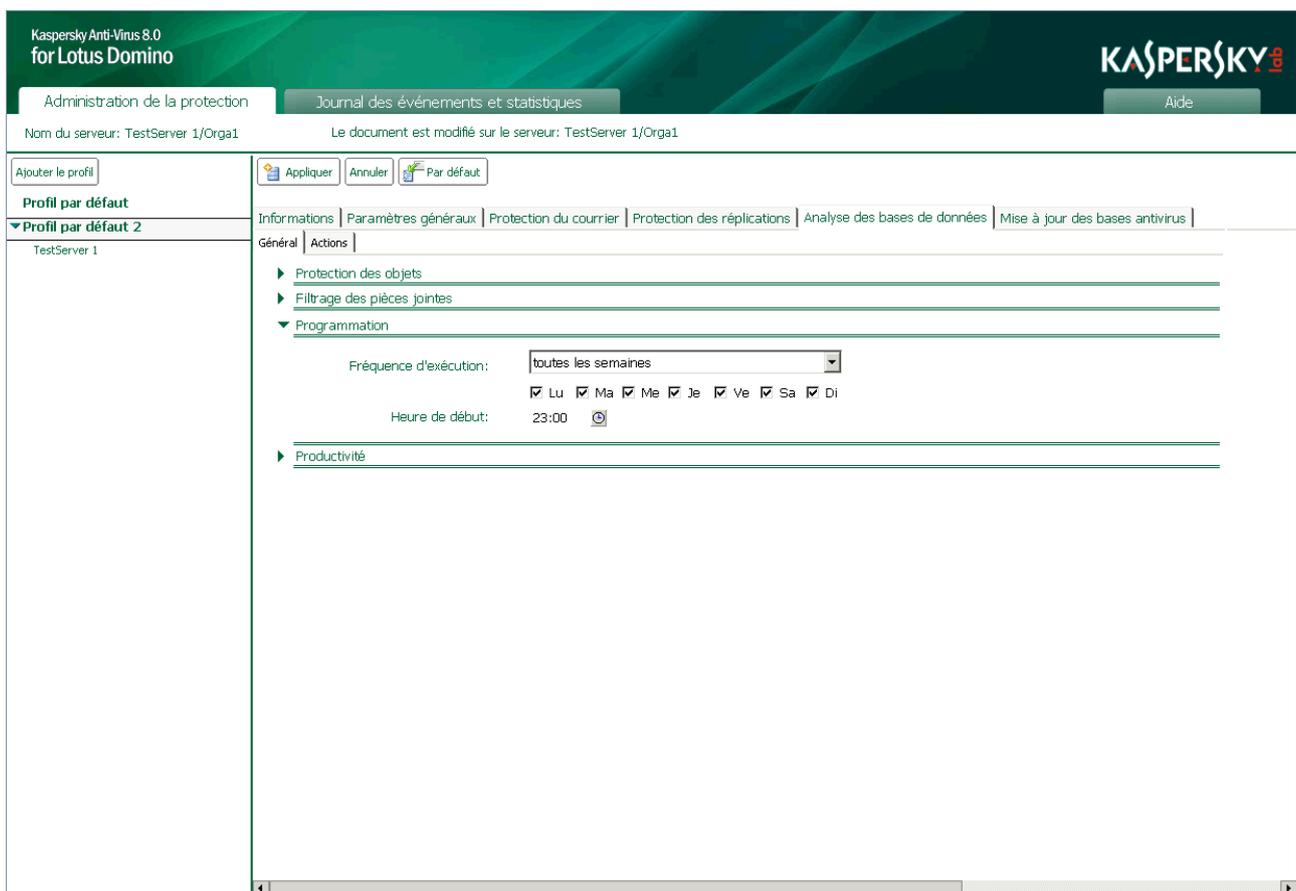


Illustration 5 : Fenêtre de la base de données Centre d'administration en mode de consultation des paramètres du profil

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

Si la case **Modifier le document sur le serveur protégé** du groupe **Administration de la configuration** du document sous l'onglet **Paramètres généraux** est cochée, alors le document est ouvert depuis une réplique de la base de données située sur le serveur correspondant à ce document de serveur.

Sur un client de la version 8 ou plus, le document est ouvert d'un clic sur le document dans le panneau de navigation.

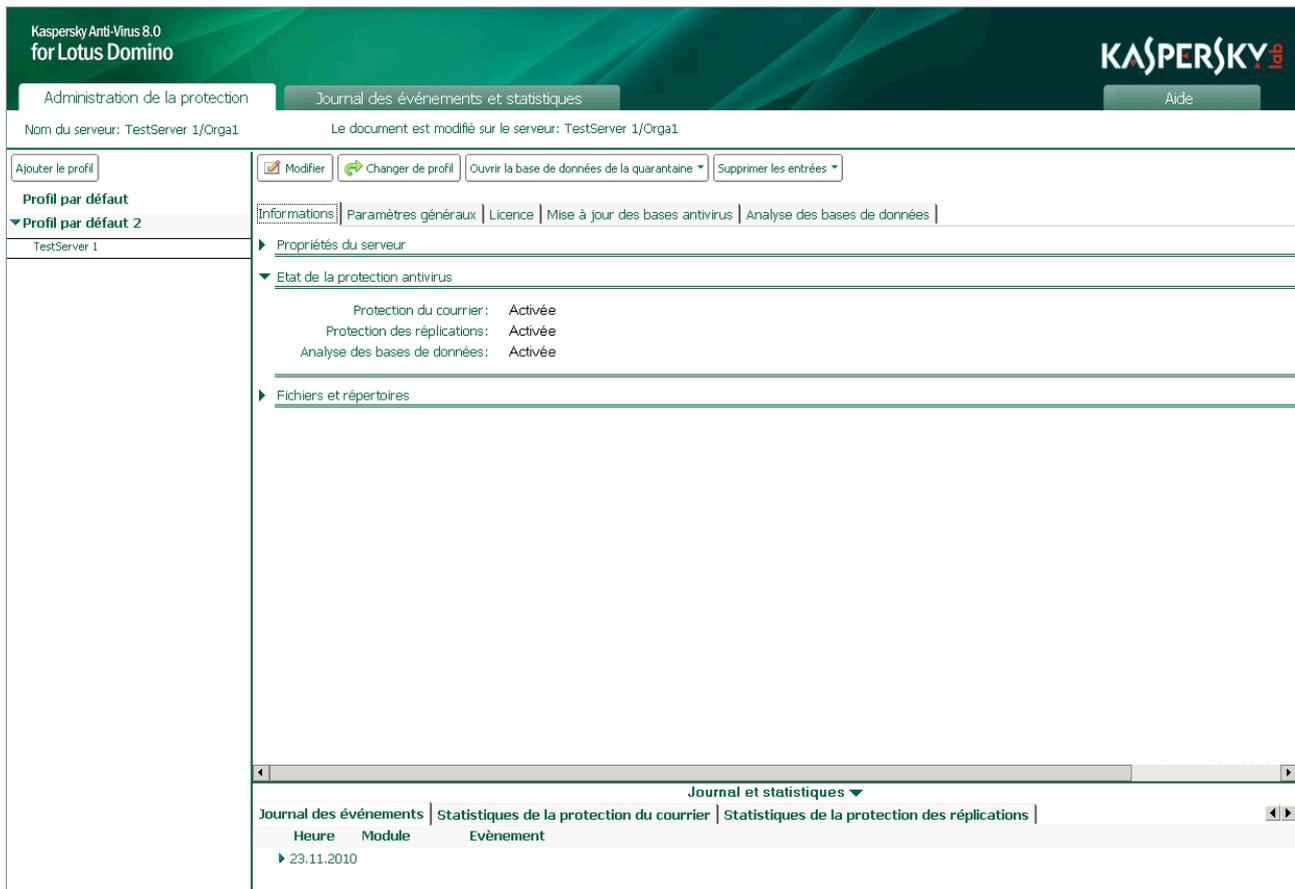


Illustration 6 : Fenêtre de la base de données Centre d'administration en mode de consultation des paramètres du serveur

Les paramètres du serveur sont présentés sur 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 composants de la protection (cf. page 45).
- **Paramètres généraux.** L'onglet reprend les paramètres de la quarantaine (cf. rubrique " Configuration des paramètres de la quarantaine " à la page 93) ainsi que les paramètres individuels du journal des événements et des statistiques pour le serveur (cf. rubrique " Configuration des paramètres du journal des événements " à la page 96).
- **Licence.** L'onglet permet d'administrer les licences (cf. rubrique " Administration des licences " à la page 32).
- **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. rubrique " Source des mises à jour " à la page 50) et du lancement de la mise à jour (cf. rubrique " Mise à jour manuelle " à la page 56).
- **Analyse des bases de données.** L'onglet permet de lancer l'analyse des bases de données manuellement pour le serveur (cf. rubrique " Analyse manuelle " à la page 85).

La partie supérieure de la zone d'administration contient le volet des actions qui regroupe les boutons de commande.

Pour modifier les paramètres du profil ou les paramètres du serveur, il faut 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 d'édition est différente de celle du mode de consultation.

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

Tableau 4. Boutons du volet des actions lors de 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 du volet des actions lors de l'utilisation des paramètres du serveur.

Tableau 5. Boutons du volet des actions lors de 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 électronique, des répliquons ou des bases de données (cf. page 88).
Supprimer les entrées	Supprimer les entrées de la quarantaine (cf. rubrique " Actions à exécuter sur les objets placés en quarantaine " à la page 91) ou du journal des événements et des statistiques pour ce serveur (cf. rubrique " Suppression des informations de la base de données Journal des événements et statistiques " à la page 101).

ONGLET JOURNAL DES ÉVÉNEMENTS ET STATISTIQUES

L'onglet **Journal des événements et statistiques** permet de travailler avec la base de données Journal des événements et statistiques : consultation des informations sur les événements enregistrés pendant l'utilisation de l'application sur tous les serveurs protégés, données statistiques sur les menaces découvertes suite à l'analyse antivirus et sur les actions exécutées sur celles-ci (cf. rubrique " Consultation de la base de données Journal des événements et statistiques " à la page [102](#)).

Sous l'onglet **Journal des événements et statistiques** dans le volet de navigation, vous trouverez la liste des rubriques et section du journal des événements et des statistiques tandis que la zone de consultation dans la partie droite de la fenêtre affiche les entrées de la base de données Journal des événements et statistiques (cf. ill. ci-après).

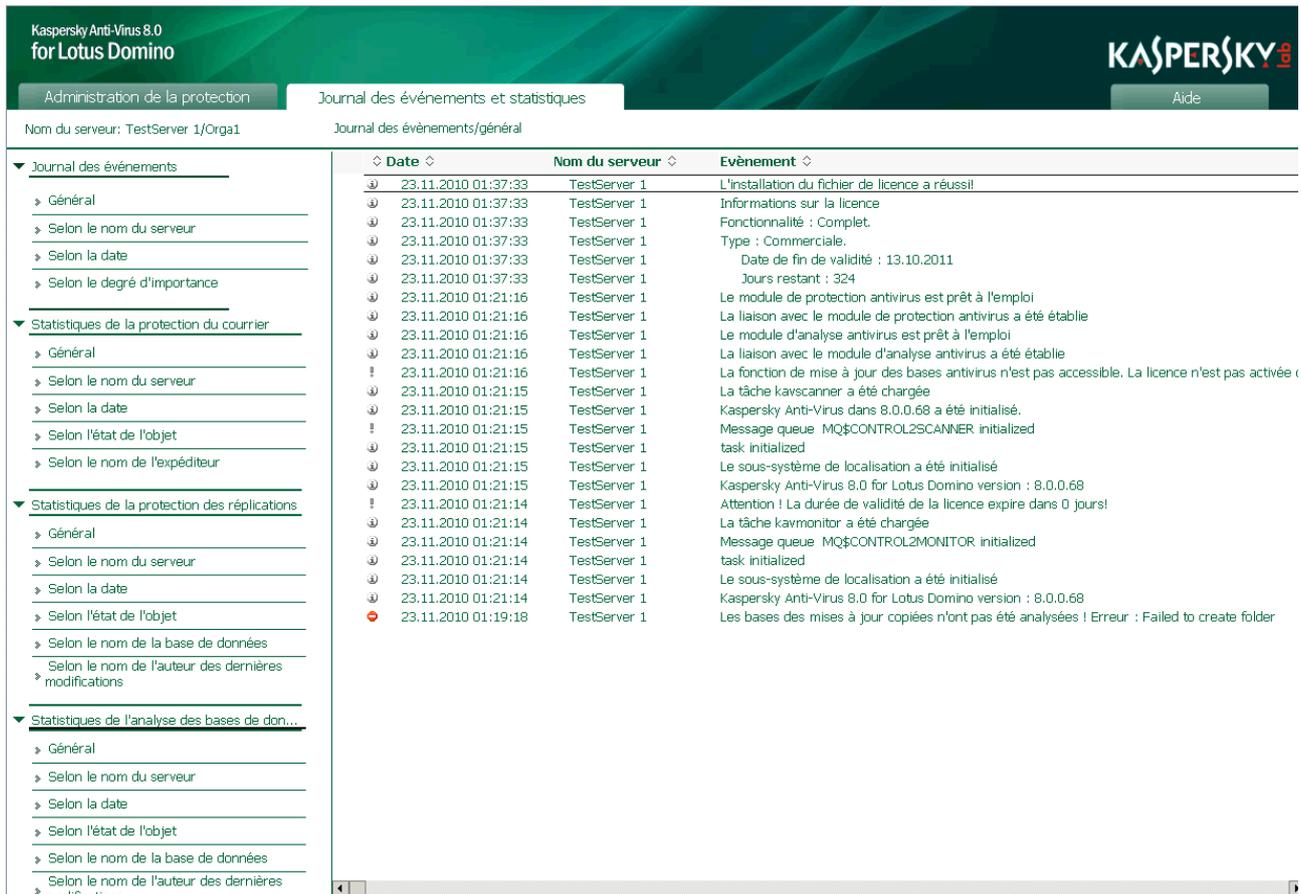


Illustration 7 : Fenêtre de la base de données Centre d'administration en mode de consultation du Journal des événements et statistiques

ONGLET AIDE

L'onglet **Aide** permet de consulter la base de données Aide.

Le panneau de navigation de l'onglet **Aide** contient la table des matières du système d'aide de Kaspersky Anti-Virus tandis que la zone de consultation de la partie droite de la fenêtre affiche le contenu de l'aide.

LANCEMENT ET ARRÊT DE L'APPLICATION

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

Vous pouvez arrêter et lancer Kaspersky Anti-Virus via la ligne de commande de la console du serveur Domino (cf. rubrique " Utilisation via la console du serveur " à la page [119](#)).

ÉTAT DE LA PROTECTION DU SERVEUR

La protection antivirus du serveur est assurée par les composants suivants : protection du courrier, protection des répliquations et analyse des bases de données. Tous les composants de la protection sont activés par défaut et sont lancés automatiquement au démarrage du serveur Domino. L'analyse des bases de données est programmée une fois par mois à 23 h 00, à partir du jour d'installation.

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur dont vous souhaitez consulter l'état de la protection.
3. Dans la zone d'administration, sélectionnez l'onglet **Informations**. L'état des composants de la protection apparaît dans le groupe **Etat de la protection antivirus** (cf. ill. ci-après).

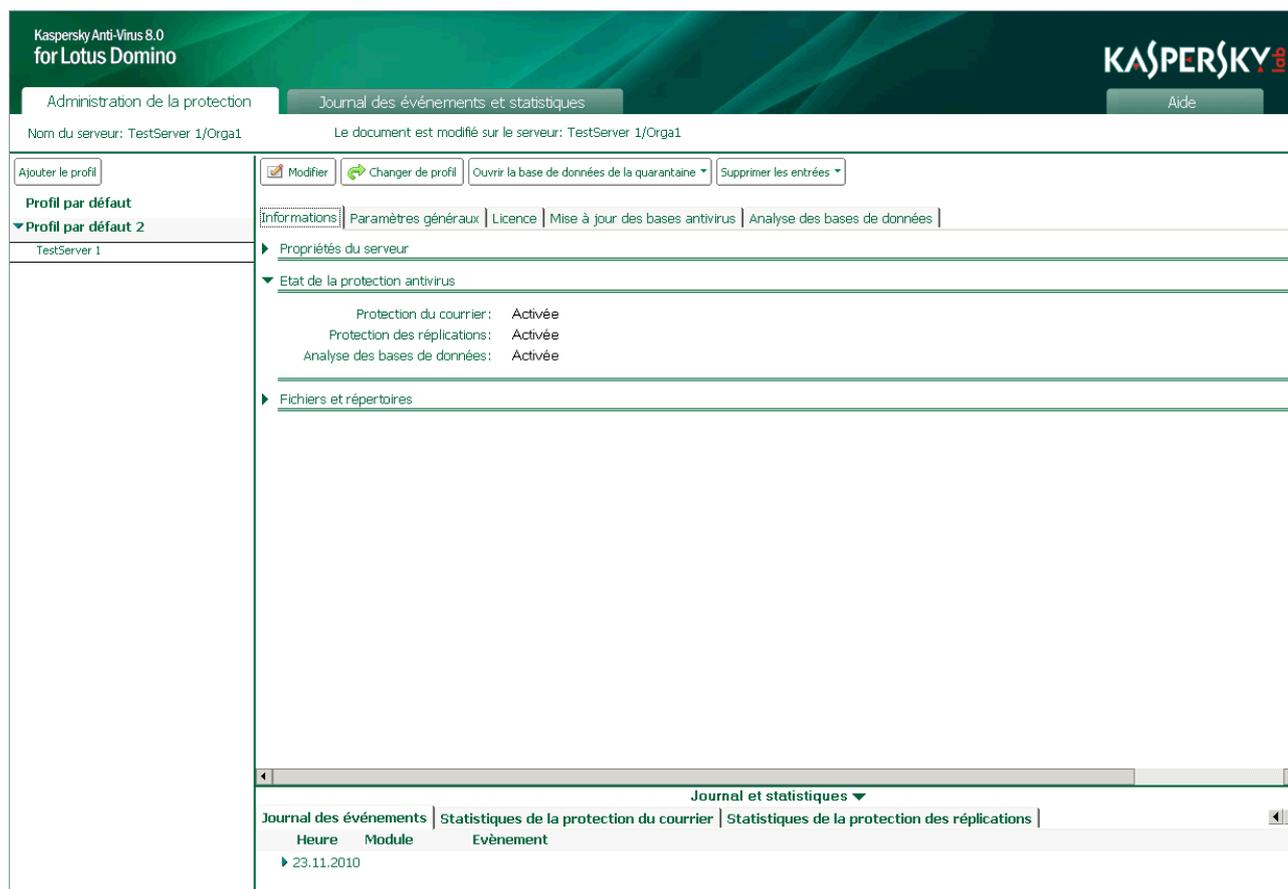


Illustration 8 : Fenêtre de la base de données Centre d'administration en mode de consultation des paramètres du serveur

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

➤ Pour activer ou désactiver un composant quelconque de la protection, procédez comme suit :

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous souhaitez activer ou désactiver un composant quelconque de la protection.

3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Informations** (cf. ill. ci-dessus).
4. Dans le groupe **Etat de la protection antivirus**, sur la ligne correspondant au composant souhaité, choisissez une des options proposées : **Activer** ou **Désactiver**.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

PROTECTION DU SERVEUR PAR DÉFAUT

La protection antivirus est active après l'installation de Kaspersky Anti-Virus et le redémarrage du serveur 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 pour l'analyse :
 - analyser le corps du message, les pièces jointes et les objets OLE ;
 - réparer les objets qui peuvent l'être, supprimer les objets irrécupérables ainsi que les objets potentiellement infectés et non analysés ;
 - analyser un objet pendant 300 ms maximum ;
 - analyser les objets d'une taille maximum de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
 - placer une copie de l'objet en quarantaine ;
 - consigner les informations sur l'objet découvert et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
 - ajouter un message informatif au corps du message ;
 - ajouter la note suivante à l'objet du message **Analysé par Kaspersky Anti-Virus for Lotus Domino**;
 - signaler le risque d'épidémie en cas de découverte de dix objets infectés en une heure.
- Analyse de tous les nouveaux documents et des documents modifiés suite à la réplication. Les valeurs suivantes sont attribuées aux paramètres pour l'analyse :
 - analyser les champs du document au format RTF, les fichiers joints et les objets OLE ;
 - réparer les objets qui peuvent l'être, supprimer les objets irrécupérables ainsi que les objets potentiellement infectés et non analysés ;
 - analyser un objet pendant 300 ms maximum ;
 - analyser les objets d'une taille maximum de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
 - placer une copie de l'objet en quarantaine ;
 - consigner les informations sur l'objet découvert et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
 - envoyer à l'administrateur les informations sur les actions exécutées.
- Analyse de la base de données. L'analyse est lancée selon une programmation, toutes les semaines à 00 h 00. Les valeurs suivantes sont attribuées aux paramètres pour l'analyse :
 - analyser les champs du document au format RTF, les fichiers joints et les objets OLE ;
 - analyser les bases de données dans la racine du répertoire data (répertoire des données du serveur Domino) et dans tous les sous-répertoires.
 - exclure de l'analyse la base de données Quarantaine ;

- réparer les objets qui peuvent l'être, supprimer les objets irréparables ainsi que les objets potentiellement infectés et non analysés ;
 - analyser un objet pendant 300 ms maximum ;
 - analyser les objets d'une taille maximum de 1 024 Ko dans la mémoire vive du serveur sans enregistrement sur le disque dur ;
 - placer une copie de l'objet en quarantaine ;
 - consigner les informations sur l'objet découvert et sur les actions exécutées dans la base de données Journal des événements et statistiques ;
 - envoyer à l'administrateur les informations sur les actions exécutées.
- Enregistre dans la base de données Journal des événements et statistiques et affiche sur la console du serveur Domino les événements survenus durant l'utilisation de Kaspersky Anti-Virus. Niveau de détail : étendu. 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.
 - Lancement de la mise à jour des bases antivirus selon la programmation tous les jours à 23 h 00. Les serveurs de Kaspersky Lab sont la source des mises à jour.

MISE À JOUR DES BASES

Kaspersky Anti-Virus recherche les programmes malveillants et répare les objets infectés à l'aide des entrées des bases antivirus. Il est primordial de maintenir l'actualité des bases antivirus car chaque jour voit l'apparition 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 livrées avec la distribution 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 utilisées par Kaspersky Anti-Virus.

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

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

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

Les mises à jour récupérées par 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 faut désigner en guise de source des mises à jour le répertoire de service kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux) sur le serveur source des mises à jour à l'adresse suivante :

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

Ainsi, si Kaspersky Anti-Virus est installé sur plusieurs serveurs, 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. rubrique " Schémas de mise à jour " à la page [51](#)).

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 sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

Avant de réaliser la mise à jour, Kaspersky Anti-Virus crée une copie de sauvegarde des bases antivirus. En cas d'interruption de la mise à jour ou si celle-ci se solde sur un échec, Kaspersky Anti-Virus restaure les bases antivirus au départ de la copie de sauvegarde. Si les bases antivirus sont endommagées pendant l'utilisation, Kaspersky Anti-Virus restaure également les bases au départ de la copie de sauvegarde créée lors de la dernière mise à jour.

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. rubrique " Journal des événements et statistiques " à la page [95](#)).

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. rubrique " Administration des paramètres de Kaspersky Anti-Virus " à la page [24](#)).

DANS CETTE SECTION

Source des mises à jour	50
Schémas de mise à jour	51
Sélection de la source de mises à jour	53
Mise à jour selon la programmation	54
Mise à jour manuelle	56

SOURCE DES MISES À JOUR

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.

Les serveurs de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour des applications de Kaspersky Lab. Il s'agit de sites Internet spéciaux qui hébergent les mises à jour de toutes les applications de Kaspersky Lab.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (ex: pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 (495) 797 87 00 ou au +7 (495) 645-79-39 pour obtenir l'adresse d'un partenaire de Kaspersky Lab qui pourra vous donner la mise à jour sur disque amovible dans un fichier zip.

Les mises à jour obtenues sur un disque amovible peuvent être placées sur un serveur FTP ou HTTP ou dans un répertoire local ou de réseau.

La source des mises à jour de Kaspersky Anti-Virus for Lotus Domino peut également être le répertoire de service kavcommon\updater\retranslation\ (kavcommon/updater/retranslation pour Linux) sur un autre serveur protégé qui accueillera les mises à jour de Kaspersky Anti-Virus installé sur ce serveur.

SCHÉMAS DE MISE À JOUR

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

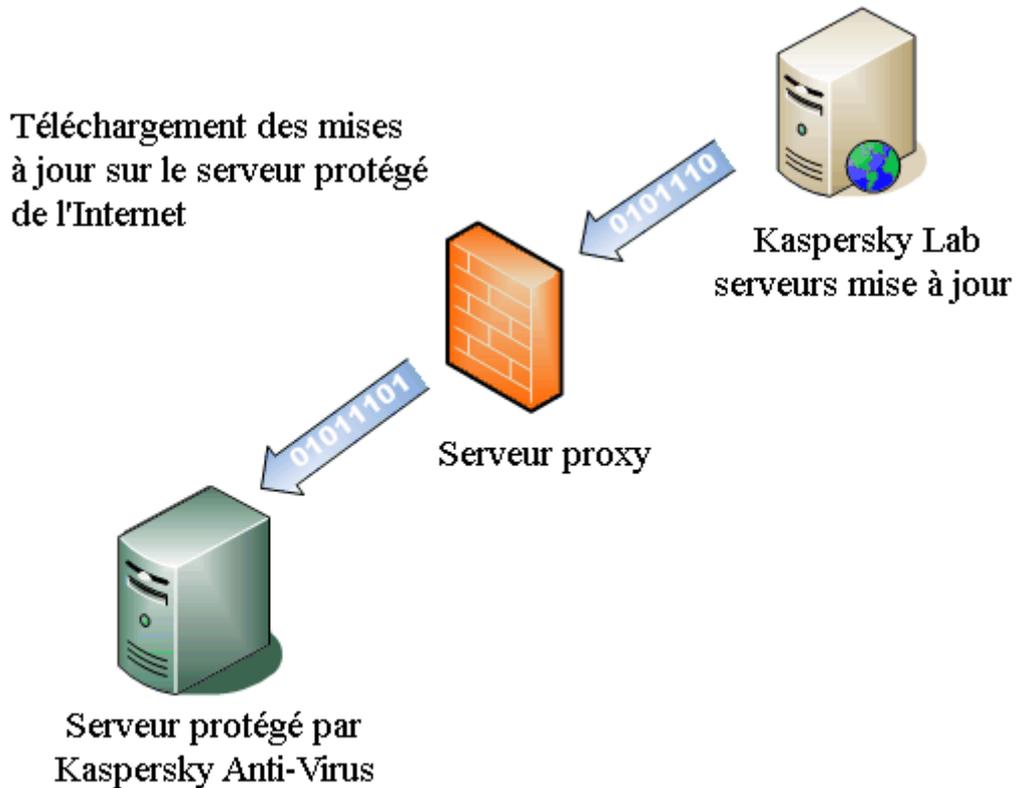


Illustration 9 : Schéma de mise à jour via Internet depuis les serveurs de Kaspersky Lab.

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 un des serveurs tandis que les autres serveurs contactent un répertoire sur ce serveur où Kaspersky Anti-Virus a placé les mises à jour récupérées (cf. ill. ci-après).

Étape 1. Téléchargement des mises à jour à partir d'Internet vers le serveur protégé sélectionné.

Étape 2. Téléchargement des mises à jour à partir d'un répertoire réseau sur le reste des serveurs protégés.

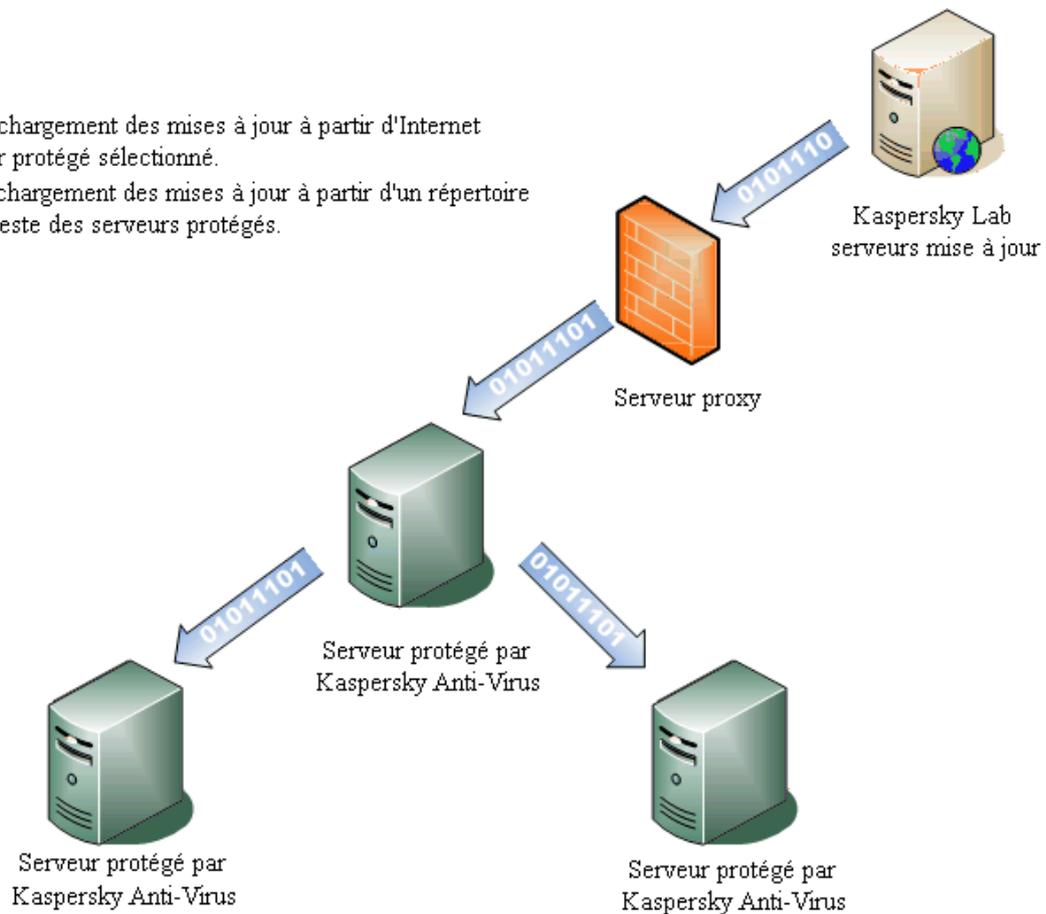


Illustration 10 : Schéma de mise à jour centralisée

➔ 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. rubrique "Sélection de la source des mises à jour" à la page 53).
2. Tous les serveurs qui recevront la mise à jour de ce serveur doivent avoir accès 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) sur le serveur ayant récupéré les mises à jour en tant que source des mises à jour pour tous les serveurs qui récupéreront les mises à jour depuis le serveur sélectionné.

En cas d'utilisation du schéma centralisé de mise à jour, il est conseillé d'utiliser la valeur suivante du paramètre KAVCustomUpdUrlOnly=1 dans notes.ini pour les serveurs qui seront mis à jour depuis le serveur sélectionné.

SÉLECTION DE LA SOURCE DE MISES À JOUR

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

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un profil si vous configurez la mise à jour pour un groupe de serveurs ou un serveur si vous configurez la mise à jour pour un serveur distinct.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et dans la zone d'administration, sélectionnez l'onglet **Mise à jour des bases antivirus** (cf. ill. ci-après).

The screenshot displays the Kaspersky Anti-Virus 8.0 for Lotus Domino administration interface. The main window title is "Kaspersky Anti-Virus 8.0 for Lotus Domino". The interface is divided into several sections:

- Top Bar:** Contains "Administration de la protection", "Journal des événements et statistiques", and "Aide".
- Server Information:** "Nom du serveur: TestServer 1/Orga1" and "Le document est modifié sur le serveur: TestServer 1/Orga1".
- Left Panel:** "Ajouter le profil", "Profil par défaut", and "Profil par défaut 2" (selected).
- Main Content Area:**
 - Buttons: "Appliquer", "Changer de profil", "Annuler", "Ouvrir la base de données de la quarantaine", "Supprimer les entrées".
 - Tabs: "Informations", "Paramètres généraux", "Licence", "Mise à jour des bases antivirus" (selected), "Analyse des bases de données".
 - Fields: "Lancement programmé précédent: 23.11.2010 01:16:06", "Prochain lancement programmé: 23.11.2010 23:00:00", "Date d'édition des bases antivirus: 06.07.2010 10:01:00".
 - Section: "Paramètres de la mise à jour".
 - Checkbox: "Utiliser les paramètres du profil" (unchecked).
 - Dropdown: "Source des mises à jour: Serveurs de mises à jour de Kaspersky Lab".
 - Checkbox: "Utiliser le serveur proxy" (checked).
 - Address: "Adresse: test".
 - Port: "Port: 1111".
 - Checkbox: "Utiliser l'authentification sur le serveur proxy" (unchecked).
 - Button: "Lancer la mise à jour".
- Bottom Panel:** "Journal et statistiques" section with a table:

Heure	Module	Evènement
23.11.2010		

Illustration 11 : Sélection de la source de la mise à jour

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 définis par le profil, cochez la case **Utiliser les paramètres du profil**.

4. Désignez la source des mises à jour. Pour ce faire, sélectionnez une des valeurs suivantes 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 serviront de source des mises à jour. Cette source est sélectionnée par défaut.
 - **Autres serveurs HTTP, FTP ou ressources de réseau** : la source des mises à jour sera la ressource désignée dans le champ **Adresse URL** (dans les paramètres du profil)/**Adresse de la source** (dans les paramètres du serveur). Désignez un serveur FTP/HTTP ou un répertoire local ou de réseau. Le chemin d'accès à la ressource doit être conforme au format UNC (Universal Naming Convention).

Les serveurs FTP avec autorisation peuvent faire office de sources des mises à jour, ce qui n'est pas le cas des serveurs HTTP avec autorisation.

Si vous souhaitez que les mises à jour soient copiées depuis le répertoire de service d'une copie de Kaspersky Anti-Virus installée sur un autre serveur protégé, saisissez dans ce champ le chemin d'accès au répertoire kavcommon\updater\retranslation (kavcommon/updater/retranslation pour Linux). Dans les systèmes d'exploitation de la famille Windows, le chemin d'accès est relatif au répertoire des fichiers binaires du serveur Domino (par défaut : C:\Program Files\IBM\Lotus\Domino). Pour les systèmes d'exploitation de la famille Linux, le chemin d'accès au répertoire est relatif au répertoire des données du serveur Domino (par défaut : /local/notesdata).

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 le serveur de mises à jour de Kaspersky Lab. Pour que le serveur soit mis à jour uniquement depuis la source de mise à jour que vous aurez désignée, il faut définir le paramètre KAVCustomUpdUrlOnly dans le fichier de configuration notes.ini (cf. rubrique " Administration des paramètres du fichier de configuration notes.ini " à la page [26](#)) : KAVCustomUpdUrlOnly=1.

5. Configurez les paramètres du serveur proxy si la connexion à la ressource 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 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. Remplissez les champs **Utilisateur** et **Mot de passe**.
6. 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 À JOUR SELON LA PROGRAMMATION

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 serveur via le profil ou utilisez les paramètres du serveur pour 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. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un profil si vous configurez la mise à jour pour un groupe de serveurs, ou un serveur si vous configurez la mise à jour pour un serveur distinct.

3. Dans le volet des actions, cliquez sur le bouton **Modifier** et dans la zone d'administration, sélectionnez l'onglet **Mise à jour des bases antivirus** (cf. ill. ci-après).

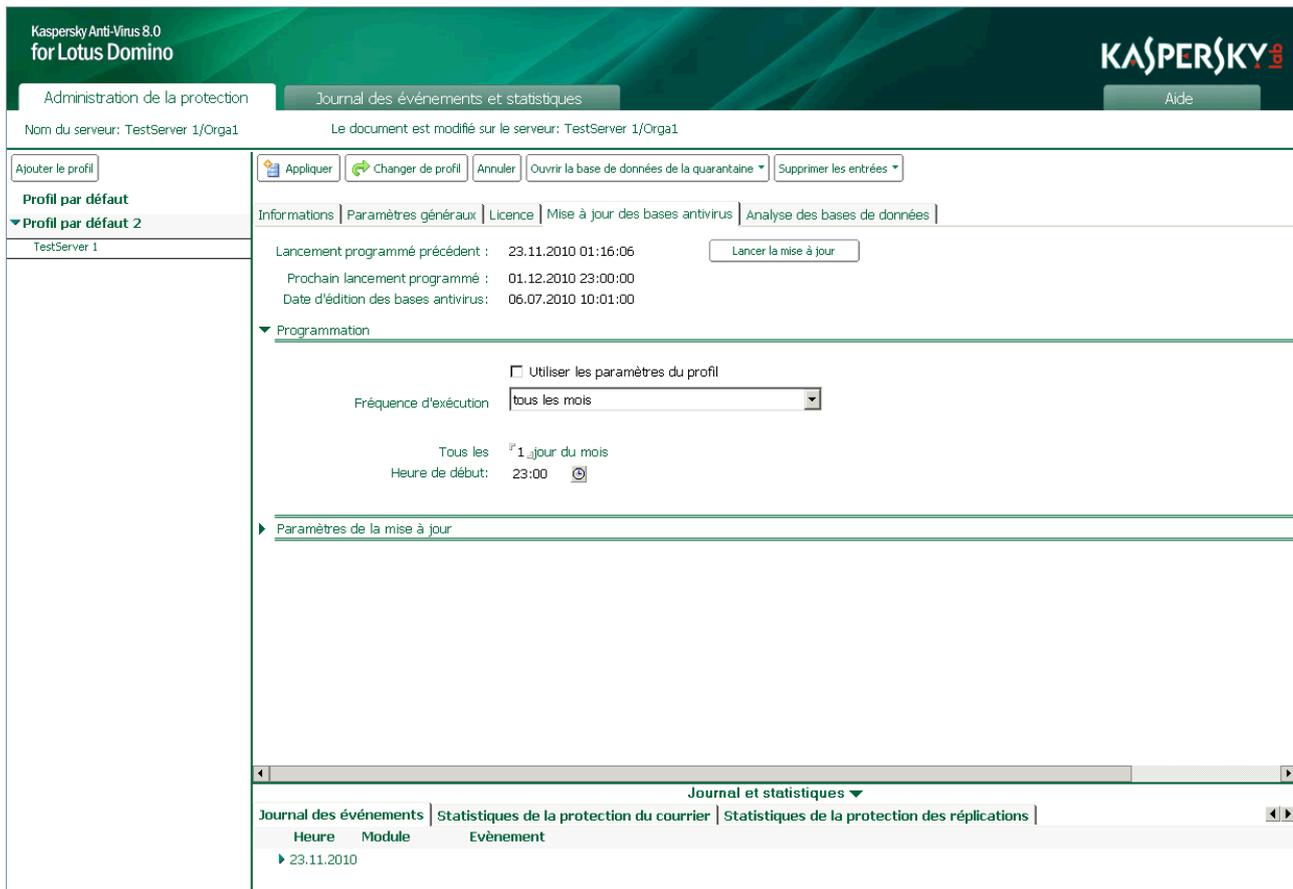


Illustration 12 : Configuration de la planification de la mise à jour des bases antivirus

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 définis par le profil, cochez la case **Utiliser les paramètres du profil**.

4. Dans le groupe **Programmation**, choisissez une des options suivantes dans la liste déroulante **Fréquence d'exécution** :
- **tous les jours**: la mise à jour aura lieu tous les jours à l'heure définie. La première exécution a lieu par défaut à 23h00.
 - **tous les mois** : la mise à jour aura lieu une fois par mois, le jour indiqué et à l'heure reprise dans le champ **Heure de début**. Saisissez l'heure souhaitée dans le champ **Heure de début**. Le format doit être - **hh:mm**.

Si le nombre de jours dans le mois est inférieur à la valeur définie, la mise jour aura lieu le dernier jour du mois.
 - **toutes les semaines** : la mise à jour aura lieu chaque semaine, le jour défini et à l'heure reprise dans le champ **Heure de début**. Cochez la case en regard des jours où la mise à jour sera lancée et saisissez l'heure souhaitée dans le champ **Heure de début**. Le format doit être - **hh:mm**.
 - **manuel** : la mise à jour programmée n'aura pas lieu. Vous pouvez lancer la mise à jour pour un serveur en particulier à l'aide du bouton **Lancer la mise à jour** (cf. rubrique " Mise à jour manuelle " à la page 56) ou via la ligne de commande (cf. rubrique " Utilisation via la console du serveur " à la page 119).

- 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 À JOUR MANUELLE

Il est possible de lancer la mise à jour manuellement 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 :

- Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
- Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel il faut actualiser les bases antivirus.
- Dans la zone d'administration, sélectionnez l'onglet **Mise à jour des bases antivirus** (cf. ill. ci-après). 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 Domino permet de suivre la progression de la mise à jour.

Illustration 13 : Sélection de la source de la mise à jour

- Cliquez sur le bouton **Lancer la mise à jour** pour lancer la mise à jour des bases antivirus pour le serveur.

La mise à jour peut également être lancée depuis la ligne de commande (cf. rubrique " Utilisation via la console du serveur " à la page [119](#)).

PROTECTION DU COURRIER

Si la protection antivirus du courrier est activée (cf. rubrique " Activation et désactivation de la protection du courrier " à la page [58](#)), Kaspersky Anti-Virus analyse et, le cas échéant, répare tous les messages du courrier entrant, sortant ou en transit qui arrivent sur le serveur 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. rubrique " Algorithme de filtrage des pièces jointes " à la page [23](#)) et l'analyse antivirus des objets (cf. rubrique " Algorithme de la recherche d'éventuelles menaces dans les objets " à la page [23](#)) a lieu.

Dans le cadre de l'analyse des messages électroniques du serveur Domino, Kaspersky Anti-Virus utilise la tâche `kavmonitor`.

Lors de l'arrêt de la tâche `kavmonitor`, l'analyse antivirus du courrier n'a pas lieu. Les messages électroniques non analysés ne sont pas transmis aux utilisateurs. Ces messages s'accumulent dans la base de données mail.box.

Pour que le courrier soit envoyé aux destinataires, le lancement de la tâche `kavmonitor` est requise.

Les messages infectés, potentiellement infectés et non analysés suite à un échec ou en raison de dégâts découverts suite à l'analyse sont traités conformément aux paramètres de la protection du courrier (cf rubrique " Actions à exécuter sur les objets du courrier " à la page [60](#)). 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. rubrique " Filtrage des pièces jointes du courrier " à la page [64](#)).

Après l'installation de l'application, ce sont les valeurs par défaut qui sont utilisées (cf. rubrique " Protection du serveur par défaut " à la page [47](#)). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Domino. 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 [88](#)).

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 sont envoyées à l'expéditeur et aux destinataires du message ainsi qu'aux administrateurs (cf. rubrique " Notifications " à la page [106](#)). 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. rubrique " Journal des événements et statistiques " à la page [95](#)).

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

Si le mécanisme de notification sur les épidémies est activé, quand le nombre d'objets infectés, potentiellement infectés et corrompus découverts et le nombre d'objets contenant la même menace augmentent, Kaspersky Anti-Virus prévient les administrateurs et ajoute les entrées de circonstance au journal des événements. Les critères pour l'envoi de notification sur les épidémies sont définis par l'administrateur (cf. rubrique " Notifications sur les épidémies " à la page [66](#)).

Vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et des corps du texte (cf. rubrique " Sélection des objets pour la protection du courrier " à la page [59](#)). Vous pouvez également limiter la durée d'analyse d'un objet afin d'accélérer la vitesse globale d'analyse des messages (cf. rubrique " Productivité " à la page [86](#)).

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. rubrique " Productivité " à la page [86](#)).

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 le serveur n'est pas prévue. Toutefois, la protection du courrier peut être désactivée (activée) uniquement pour chaque serveur pris séparément (cf. rubrique " Activation et désactivation de la protection du courrier " à la page [58](#)).

N'oubliez pas les restrictions suivantes dans l'utilisation de l'application :

- Il est impossible de détecter des menaces dans les messages cryptés par la 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 sur l'analyse ou par le remplacement des fichiers joints par des fichiers réparés.
- Avant l'analyse antivirus, les messages au format MIME sont convertis au format Rich Tex. Dans ce cas, la mise en page du message peut être modifiée.

DANS CETTE SECTION

Activation et désactivation de la protection du courrier.....	58
Sélection des objets pour la protection du courrier.....	59
Actions à exécuter sur les objets du courrier.....	60
Filtrage des pièces jointes du courrier.....	64
Notifications sur les épidémies.....	66

ACTIVATION ET DÉSACTIVATION DE LA PROTECTION DU COURRIER

La protection du courrier est activée par défaut et elle est lancée au démarrage du serveur 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.

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

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous voulez désactiver la protection du courrier.

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

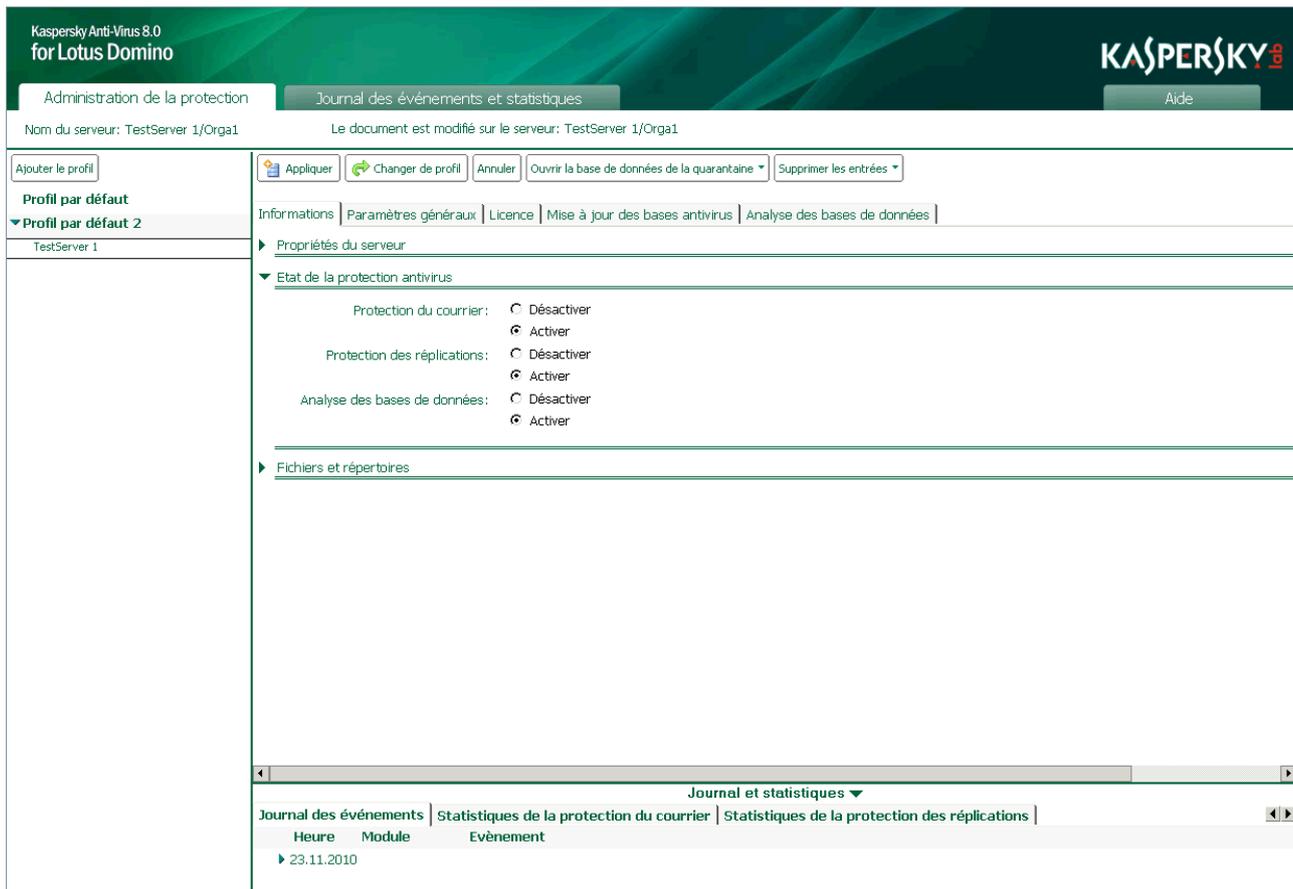


Illustration 14: Activation/désactivation de la protection du courrier

4. Dans le groupe **Etat de la protection antivirus**, sur la ligne **Protection du courrier** (cf. ill. ci-dessus), choisissez l'option voulue : **Activer** ou **Désactiver**.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

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

► Pour sélectionner les objets à protéger, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

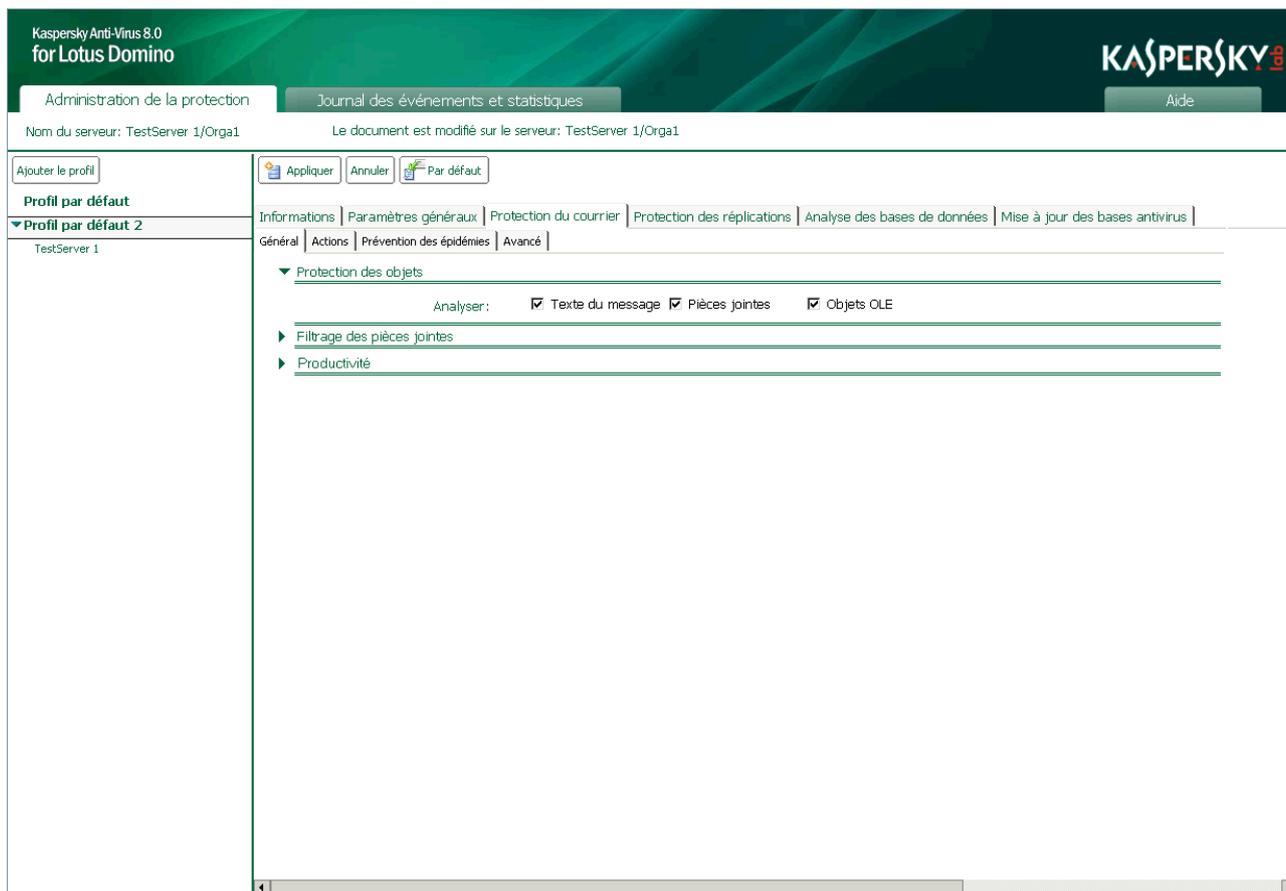


Illustration 15 : Sélection des objets de la protection du courrier

4. Dans le groupe **Protection des objets**, cochez les cases suivantes pour pouvoir analyser les objets :
 - **Pièces jointes** : analyser tout fichier joint au message.
 - **Objets OLE** : analyser tous les objets OLE intégrés au message.
 - **Texte du message** : analyser le corps du message.

Si la case n'est pas cochée, l'analyse des objets correspondant n'aura pas lieu.

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

ACTIONS À EXÉCUTER 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. rubrique " Traitement des objets et actions exécutées sur ceux-ci " à la page 24). Les objets sains sont transmis sans aucune modification au système de messagerie. Les actions à exécuter sur les objets réparables, irréparables, potentiellement infectés et non analysés sont définies par l'administrateur. Les actions qui seront exécutées par l'application sont définies pour chaque état individuel.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme réparable, Kaspersky Anti-Virus le répare et l'objet réparé est transmis au système de messagerie.

- Si l'objet est considéré comme irréparable, Kaspersky Anti-Virus le supprime du message.
- 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 prévu pour l'analyse s'est écoulé), Kaspersky Anti-Virus supprime l'objet du message.

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 découverts et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques (cf. rubrique " Journal des événements et statistiques " à la page [95](#)).

Après l'analyse antivirus de tous les objets qui composent le message et l'exécution des actions requises, le message dans son ensemble peut être soumis à une des actions complémentaires suivantes :

- 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) ;
- Transfert d'une copie du message d'origine complet dans la base de données Quarantaine (option désactivée par défaut).

➔ Pour configurer les actions à exécuter sur les objets, 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 modifier les paramètres.
3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier**, sélectionnez l'onglet **Actions** (cf. ill. ci-après).

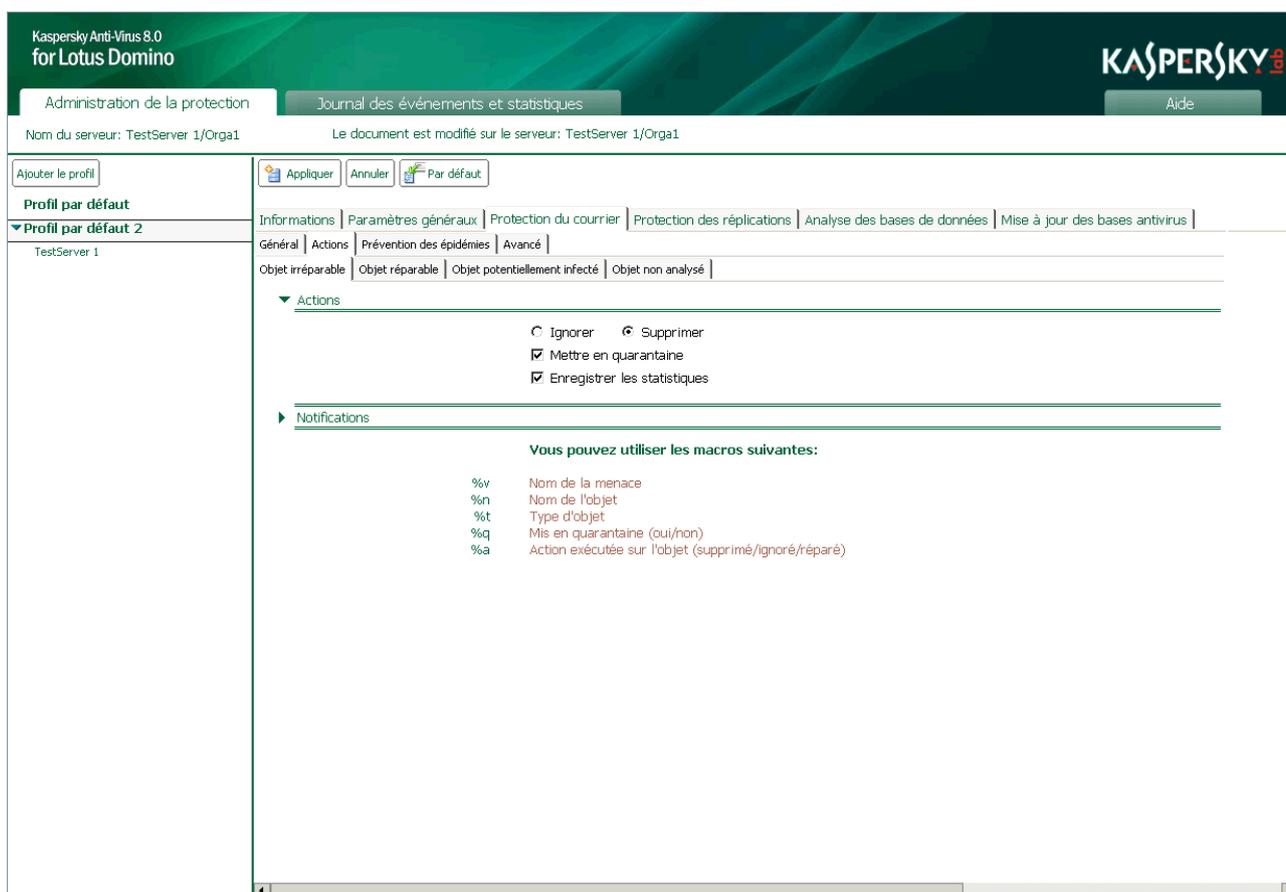


Illustration 16: Configuration des actions à exécuter sur les objets irréparables dans le cadre de la protection du courrier

4. Sous l'onglet **Actions**, sélectionnez l'onglet correspondant à l'état de l'objet dont vous souhaitez configurer le traitement. Vous avez le choix parmi les onglets suivants :
 - **Objet irréparable** : configuration des paramètres de traitement des objets irréparables.
 - **Objet réparable** : configuration des paramètres de traitement des objets réparables.
 - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
 - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.
5. Dans le groupe **Actions** (cf. ill. ci-dessus), sélectionnez l'action à exécuter sur l'objet détecté et, le cas échéant, cochez les cases suivantes :
 - **Mettre en quarantaine** : avant le traitement, une copie de l'objet sera placée dans la base de données Quarantaine.

Si dans les paramètres de protection du courrier sous l'onglet **Avancé**, la case **Mettre le message complet en quarantaine** est cochée, alors l'enregistrement complémentaire des parties de l'objet n'aura pas lieu. Après l'analyse de tous les objets qui composent le message, une copie du message original sera placée en entier dans la base de données Quarantaine, avec toutes les pièces jointes. Si la case **Mettre le message complet en quarantaine** n'est pas cochée, alors seul l'objet sera mis en quarantaine ; le message dont il fait partie ne sera pas mis en quarantaine.

- **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées dans les sources définies par le champ **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs sources de conservation des informations sont sélectionnées simultanément, l'écriture sera réalisée simultanément dans les lieux de stockage des informations indiqués.
 - **Sur la console** (journal système Domino log.nsf) ;
 - **Dans le journal** ;
 - **Dans le fichier** (nom du fichier par défaut : server.log_N, où N est le numéro de séquence du log).

6. Dans le groupe **Notifications** (cf. ill. ci-après), configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. rubrique " Notifications " à la page [106](#)).

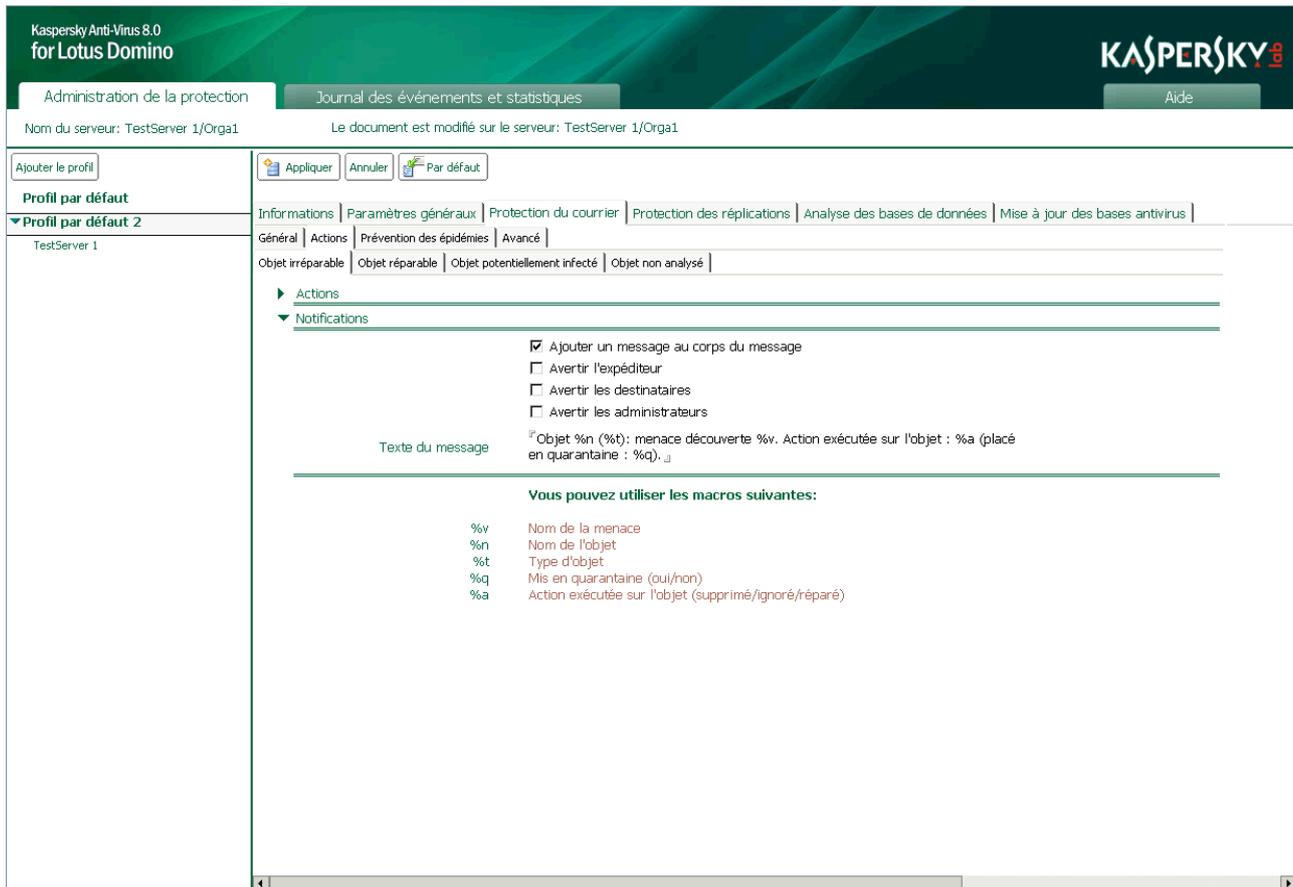


Illustration 17 : Configuration des notifications

7. 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 après l'analyse du message et de tous ses composants, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier**, sélectionnez l'onglet **Avancé** (cf. ill. ci-après).

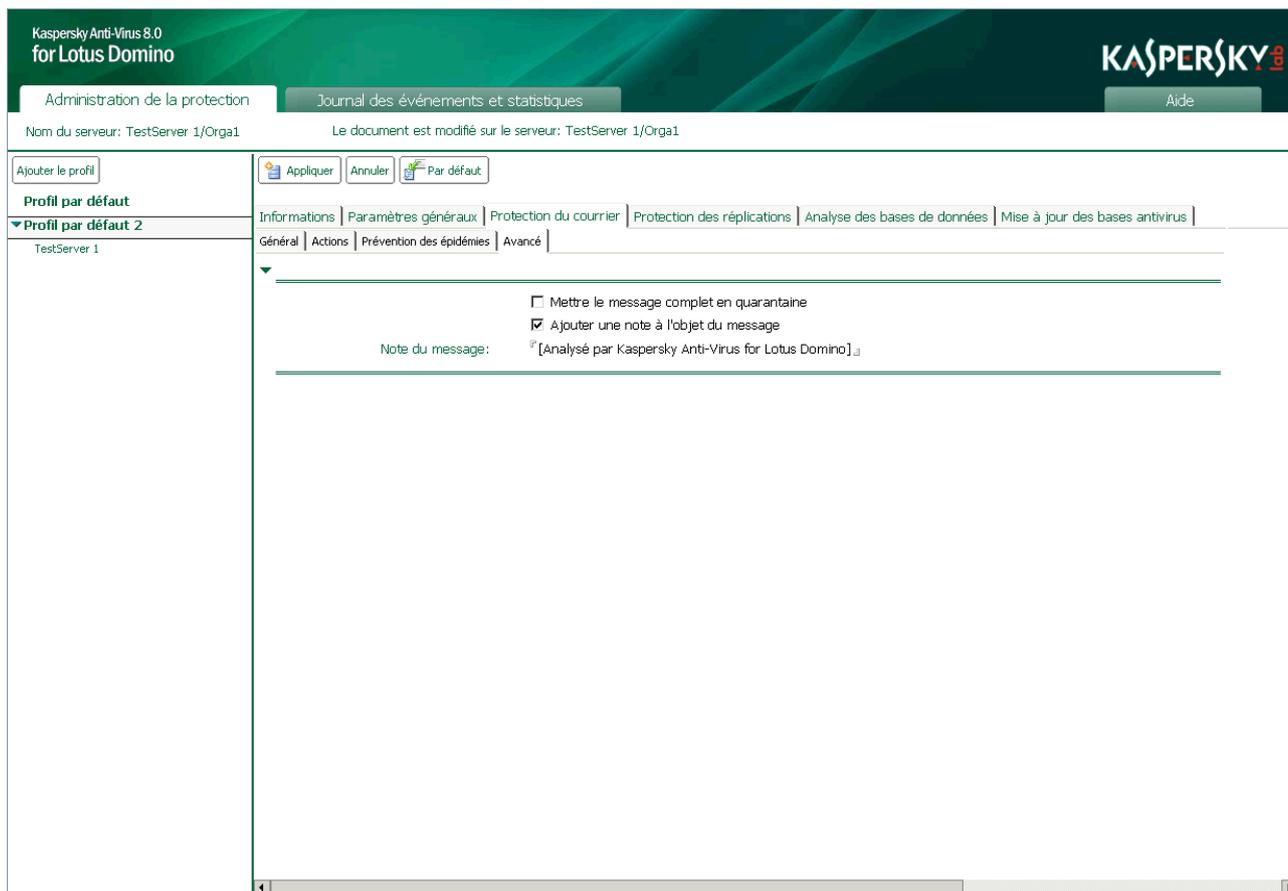


Illustration 18 : Configuration des actions à exécuter après l'analyse des messages

4. Sous l'onglet **Avancé**, procédez comme suit :
 - Cochez la case **Mettre le message complet en quarantaine**. Après l'analyse de tous les objets qui composent le message, une copie du message d'origine sera conservée en entier dans la base de données Quarantaine, avec toutes les pièces jointes.
 - Cochez la case **Ajouter une note à l'objet du message** et dans le champ **Note du message**, rédigez le texte qui sera ajouté à l'objet du message analysé. Par défaut, le champ **Note du message** contient la valeur **Analysé par Kaspersky Anti-Virus for Lotus Domino**.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

FILTRAGE DES PIÈCES JOINTES DU COURRIER

Kaspersky Anti-Virus peut filtrer les objets joints aux messages (cf. rubrique " Algorithme de filtrage des pièces jointes " à la page 23). 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 n'est pas activé par défaut dans la protection du courrier.

➔ Pour configurer le filtrage des pièces jointes, 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 modifier les paramètres.

- Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

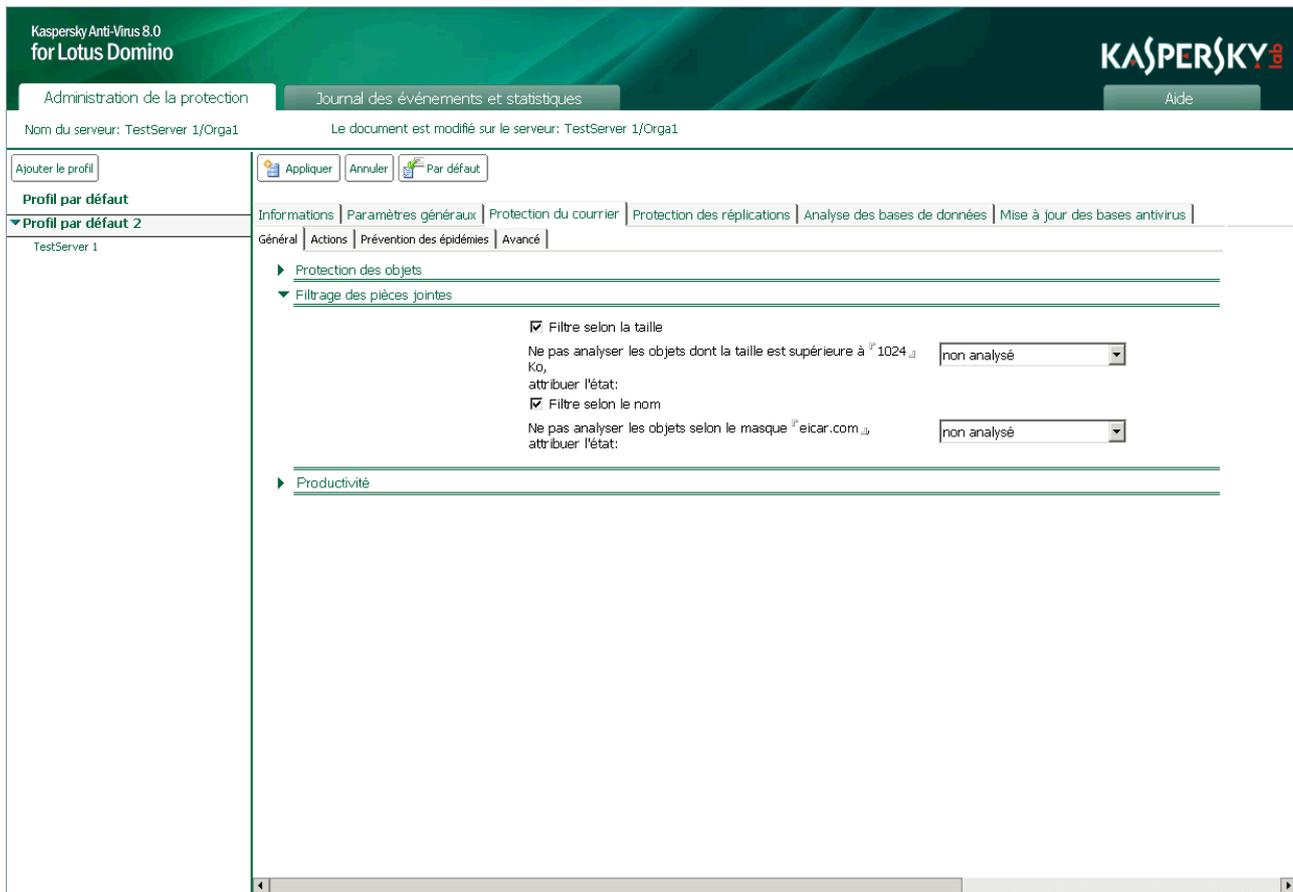


Illustration 19 : Configuration des paramètres de filtrage des pièces jointes des messages

- Dans le groupe **Filtrage des pièces jointes**, cochez les cases suivantes et définissez les paramètres correspondants si vous souhaitez filtrer les objets :
 - 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 est supérieure à**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera filtré et exclu de l'analyse antivirus. Dans la liste déroulante, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus. La valeur sélectionnée par défaut 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, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus. La valeur sélectionnée par défaut est *non analysé*.

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

Vous pouvez désigner plusieurs masques 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, ne sera 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, ne sera analysé. Par contre, le fichier abc12345.exe sera analysé.

Si la case n'est pas cochée, le filtrage des objets correspondant n'aura pas lieu.

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

NOTIFICATIONS SUR LES ÉPIDÉMIES

Kaspersky Anti-Virus peut prévenir l'administrateur en cas d'augmentation du nombre d'objets infectés, potentiellement infectés et endommagés, découverts pendant l'analyse des messages et signale également le nombre d'objets contenant la même menace.

Pour chaque catégorie citée, Kaspersky Anti-Virus enregistre le nombre total d'objets découverts au cours d'une période définie et si ce nombre dépasse la valeur maximale autorisée, il prévient l'administrateur du serveur et les administrateurs de profil et ajoute l'entrée de rigueur au journal des événements.

Cette possibilité peut-être utile lors des épidémies de virus et permet à l'administrateur de réagir en temps opportuns lorsque la menace d'une attaque de virus se manifeste.

Les administrateurs de serveur sont désignés dans les paramètres du serveur (cf. rubrique " Désignation de l'administrateur de serveur " à la page [111](#)) : sous l'onglet **Informations** dans le groupe **Propriétés du serveur**. Les administrateurs de profil sont désignés dans les paramètres du profil (cf. rubrique " Désignation de l'administrateur de profil " à la page [111](#)) : sous l'onglet **Paramètres généraux** dans le groupe **Sécurité**.

Les paramètres de notification sur les menaces d'épidémie sont définis dans les paramètres de protection du courrier pour chaque catégorie d'objet séparément.

► *Pour configurer les paramètres de notification sur les épidémies, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier**, sélectionnez l'onglet **Prévention des épidémies** (cf. ill. ci-après).

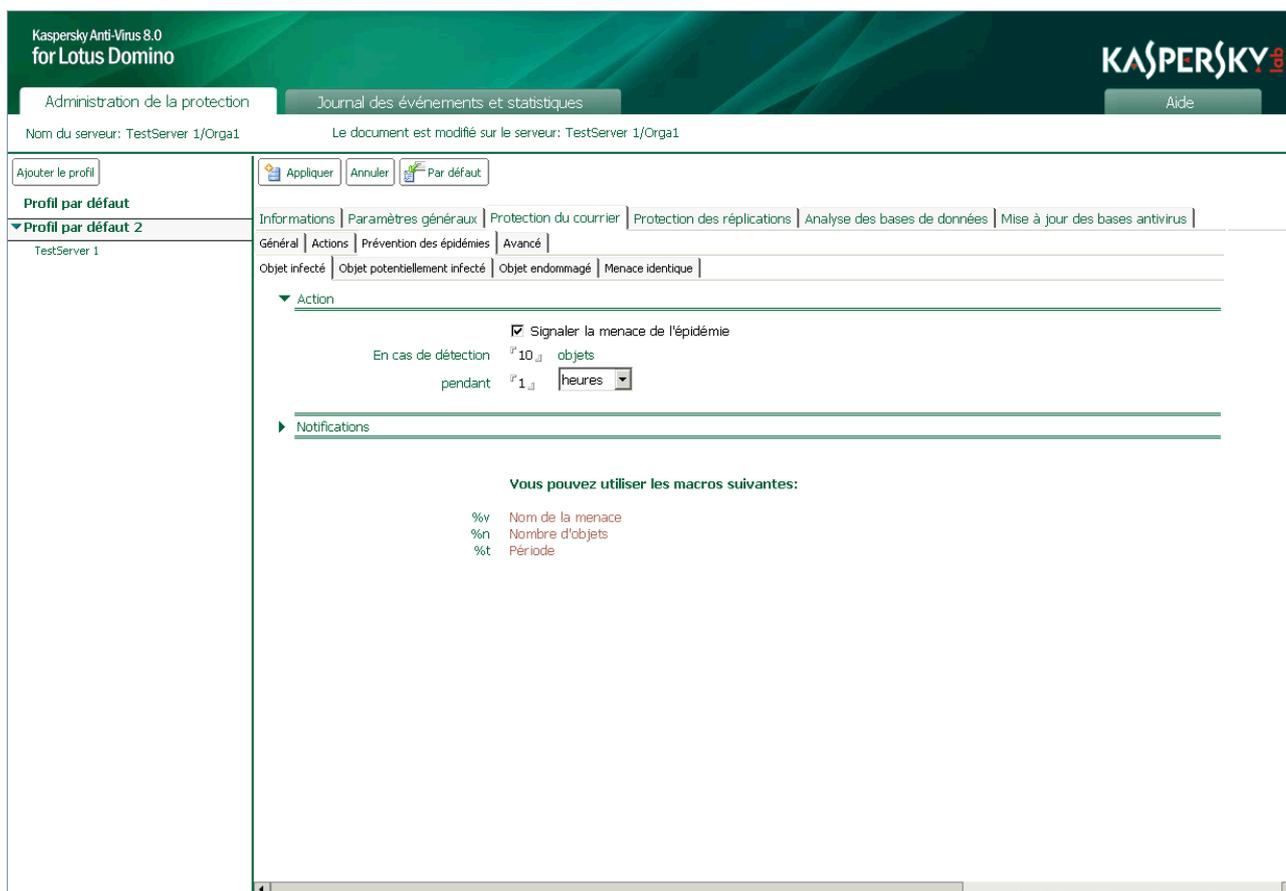


Illustration 20 : Configuration des notifications sur les épidémies

4. Sous l'onglet **Prévention des épidémies**, sélectionnez l'onglet correspondant à la catégorie d'objets pour laquelle vous souhaitez configurer les paramètres de notification sur les épidémies. Vous avez le choix parmi les onglets suivants :
 - **Objet infecté** : configuration des paramètres de notification sur le dépassement de la valeur maximum autorisée d'objets infectés découverts (réparables et irréparables compris).
 - **Objet potentiellement infecté** : configuration des paramètres de notification sur le dépassement du nombre maximum autorisé d'objets potentiellement infectés découverts.
 - **Objet endommagé** : configuration des paramètres de notification sur le dépassement du nombre autorisé d'objets non analysés découverts.
 - **Menace identique** : configuration des paramètres de notification sur le dépassement du nombre autorisé d'objets contenant la même menace.
5. Dans le groupe **Action** (cf. ill. ci-dessus), cochez la case **Signaler la menace d'épidémie** afin d'activer le mécanisme de prévention des épidémies et définissez les valeurs des paramètres selon lesquels la notification sera réalisée : nombre maximal d'objets autorisés et intervalle de temps au cours duquel ils ont été découverts.
6. Dans le groupe **Notifications** (cf. ill. ci-dessus), saisissez dans le champ **Texte du message** le texte du message de notification qui sera envoyé à l'adresse de courrier électronique des administrateurs. Vous pouvez utiliser les champs suivants :
 - **%v** : nom de la menace découverte dans l'objet ;
 - **%n** : nombre d'objets ;

- %t : période au cours de laquelle les objets ont été découverts.

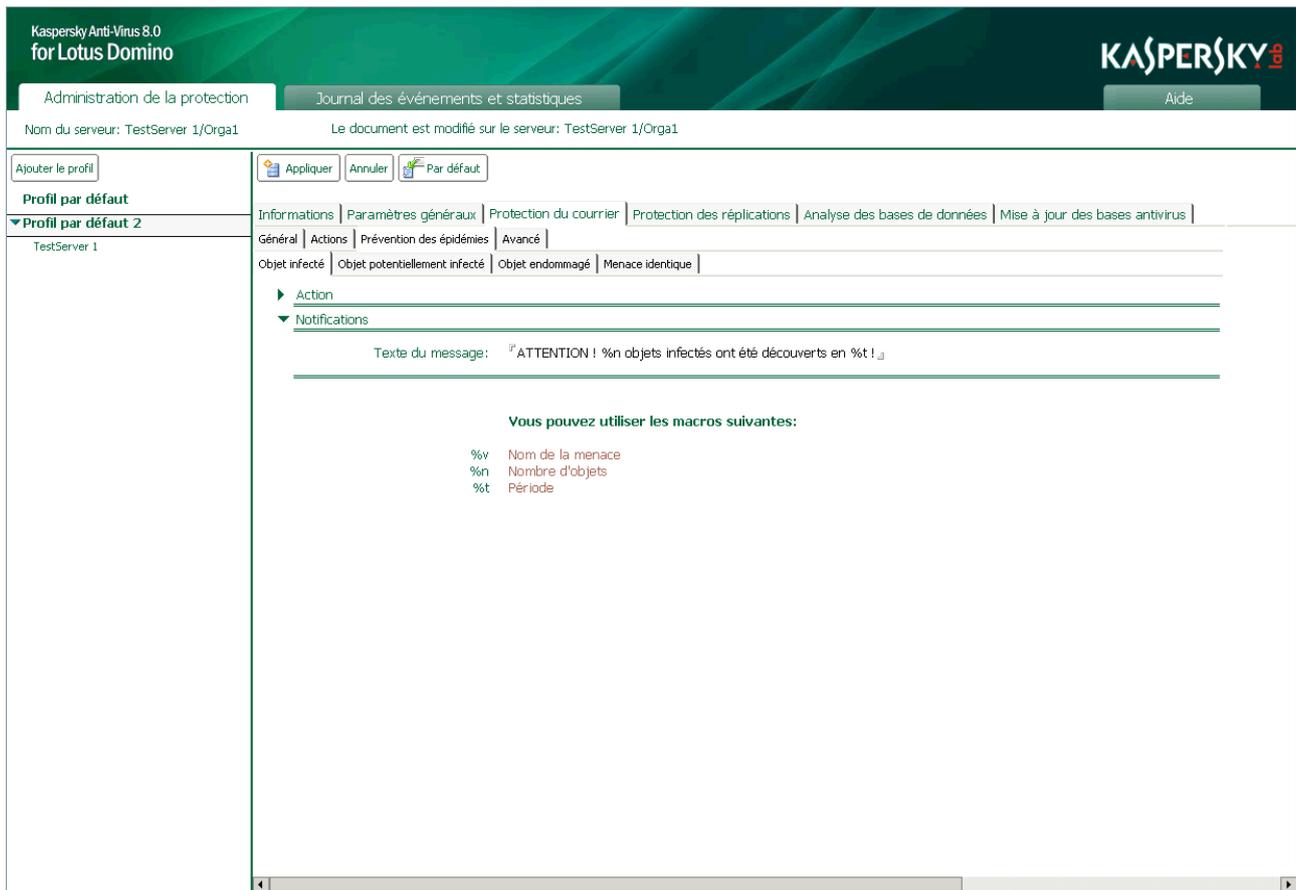


Illustration 21 : Rédaction du texte de la notification

7. 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 RÉPLICATIONS

Si la protection antivirus des répliques est activée (cf. rubrique " Activation et désactivation de la protection des répliques " à la page [70](#)), Kaspersky Anti-Virus analyse les documents placés sur le serveur protégé et qui ont été modifiés suite à la réplique. Le contenu des champs du document au format Rich Texte, les fichiers inclus dans le document et les objets OLE intégrés sont soumis à la recherche d'éventuelles menaces. Les répliques sortantes ne sont pas analysées.

Les objets infectés, potentiellement infectés et non analysés suite à un échec ou en raison de dégâts découverts suite à l'analyse sont traités conformément aux paramètres de la protection des répliques (cf rubrique " Actions à exécuter sur les objets en mode de protection des répliques " à la page [72](#)).

Après l'installation de l'application, ce sont les valeurs par défaut qui sont utilisées (cf. rubrique " Protection du serveur par défaut " à la page [47](#)). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Domino. Une partie des paramètres cités ici est désactivée par défaut ou peut être désactivée par l'administrateur.

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. rubrique " Filtrage des pièces jointes en mode de protection des répliques " à la page [74](#)).

Avant le traitement de l'objet une copie est placée par défaut en quarantaine (cf. page [88](#)). Le document auquel il appartient 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. rubrique " Notifications " à la page [106](#)). 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. rubrique " Journal des événements et statistiques " à la page [95](#)).

Le cas échéant, vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et du contenu des champs (cf. rubrique " Sélection des objets de la protection des répliques " à la page [71](#)). Vous pouvez également limiter la durée d'analyse d'un objet afin d'accélérer la vitesse globale d'analyse des répliques (cf. rubrique " Productivité " à la page [86](#)).

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. rubrique " Productivité " à la page [86](#)).

Les paramètres de la protection des répliques sont définis par le profil auquel appartient le serveur protégé. La configuration de paramètres individuels de la protection des répliques pour le serveur n'est pas prévue. Toutefois, la protection des répliques peut être désactivée (activée) uniquement pour chaque serveur pris séparément (cf. rubrique " Activation et désactivation de la protection des répliques " à la page [70](#)).

DANS CETTE SECTION

Activation/désactivation de la protection des répliques.....	70
Sélection des objets de la protection des répliques	71
Actions à exécuter sur les objets en mode de protection des répliques.....	72
Filtrage des pièces jointes en mode de protection des répliques.....	74

ACTIVATION/DÉSACTIVATION DE LA PROTECTION DES RÉPLICATIONS

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

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

➔ Pour activer ou désactiver la protection des réplifications, procédez comme suit.

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous voulez désactiver la protection des réplifications.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Informations** (cf. ill. ci-après).

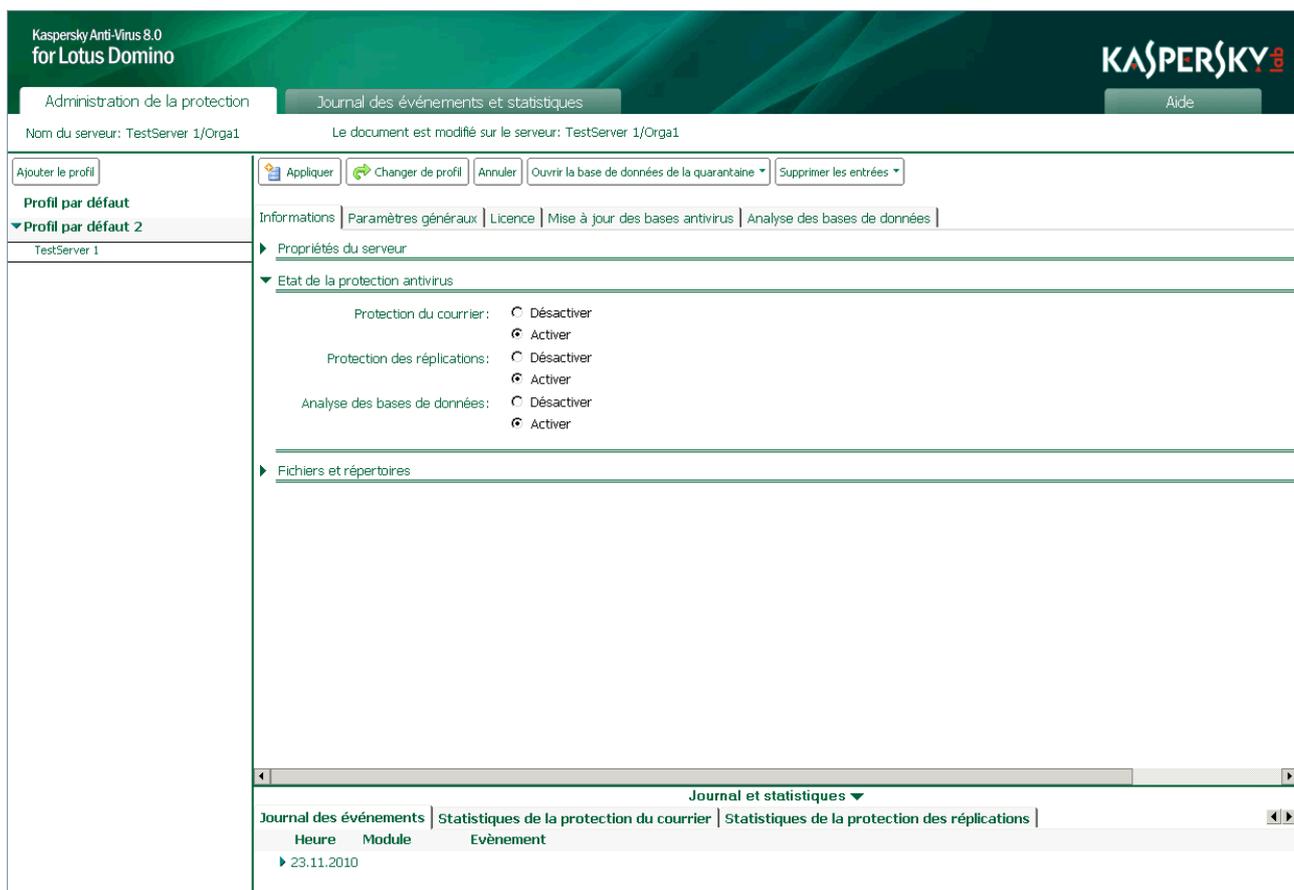


Illustration 22 : Activation/désactivation de la protection des réplifications

4. Dans le groupe **Etat de la protection antivirus**, sur la ligne **Protection des réplifications** (cf. ill. ci-dessus), choisissez l'option voulue : **Activer** ou **Désactiver**.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

SÉLECTION DES OBJETS DE LA PROTECTION DES RÉPLICATIONS

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

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

► Pour sélectionner les objets à protéger, 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 modifier les paramètres.
3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection des répliquions**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

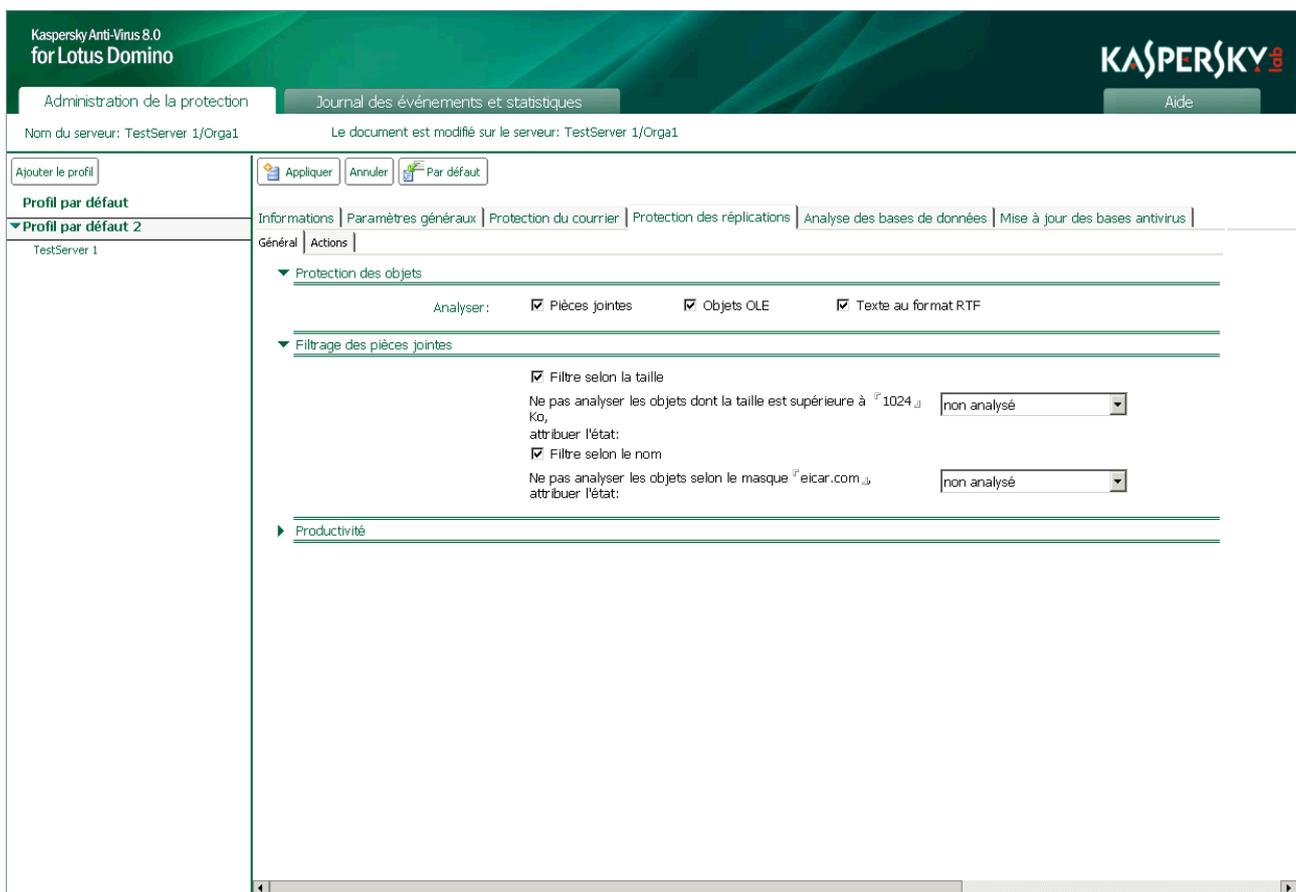


Illustration 23 : Sélection des objets de la protection des répliquions

4. Dans le groupe **Protection des objets**, cochez les cases suivantes pour pouvoir analyser les objets :
 - **Pièces jointes** : analyser tout fichier joint au document.
 - **Objets OLE** : analyser tous les objets OLE intégrés au document.

- **Texte au format RTF** : analyser les champs du document au format Rich Text.

Si la case n'est pas cochée, l'analyse des objets correspondant n'aura pas lieu.

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

ACTIONS À EXÉCUTER SUR LES OBJETS EN MODE DE PROTECTION DES RÉPLICATIONS

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite à l'analyse antivirus et suite au filtrage des pièces jointes (cf. rubrique " Traitement des objets et actions exécutées sur ceux-ci " à la page [24](#)). Les objets sains restent dans le document sans aucune modification. Les actions à exécuter sur les objets réparables, irréparables, potentiellement infectés et non analysés sont définies par l'administrateur. Les actions qui seront exécutées par l'application sont définies pour chaque état individuel.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme réparable, Kaspersky Anti-Virus le répare. L'objet réparé est conservé dans le document à l'adresse d'origine.
- Si l'objet est considéré comme irréparable, Kaspersky Anti-Virus le supprime du document.
- 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 prévu pour l'analyse s'est écoulé), Kaspersky Anti-Virus supprime l'objet du document.

Par défaut, une copie de l'objet est placée dans la base de données Quarantaine avant la réparation ou la suppression. Les informations sur les objets découverts et les actions exécutées peuvent être envoyées aux administrateurs (cf. rubrique " Notifications " à la page [106](#)) et conservées dans la base de données Journal des événements et statistiques (cf. rubrique " Journal des événements et statistiques " à la page [95](#)).

► *Pour configurer les paramètres de traitement des objets, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection des répliquions**, sélectionnez l'onglet **Actions** (cf. ill. ci-après).

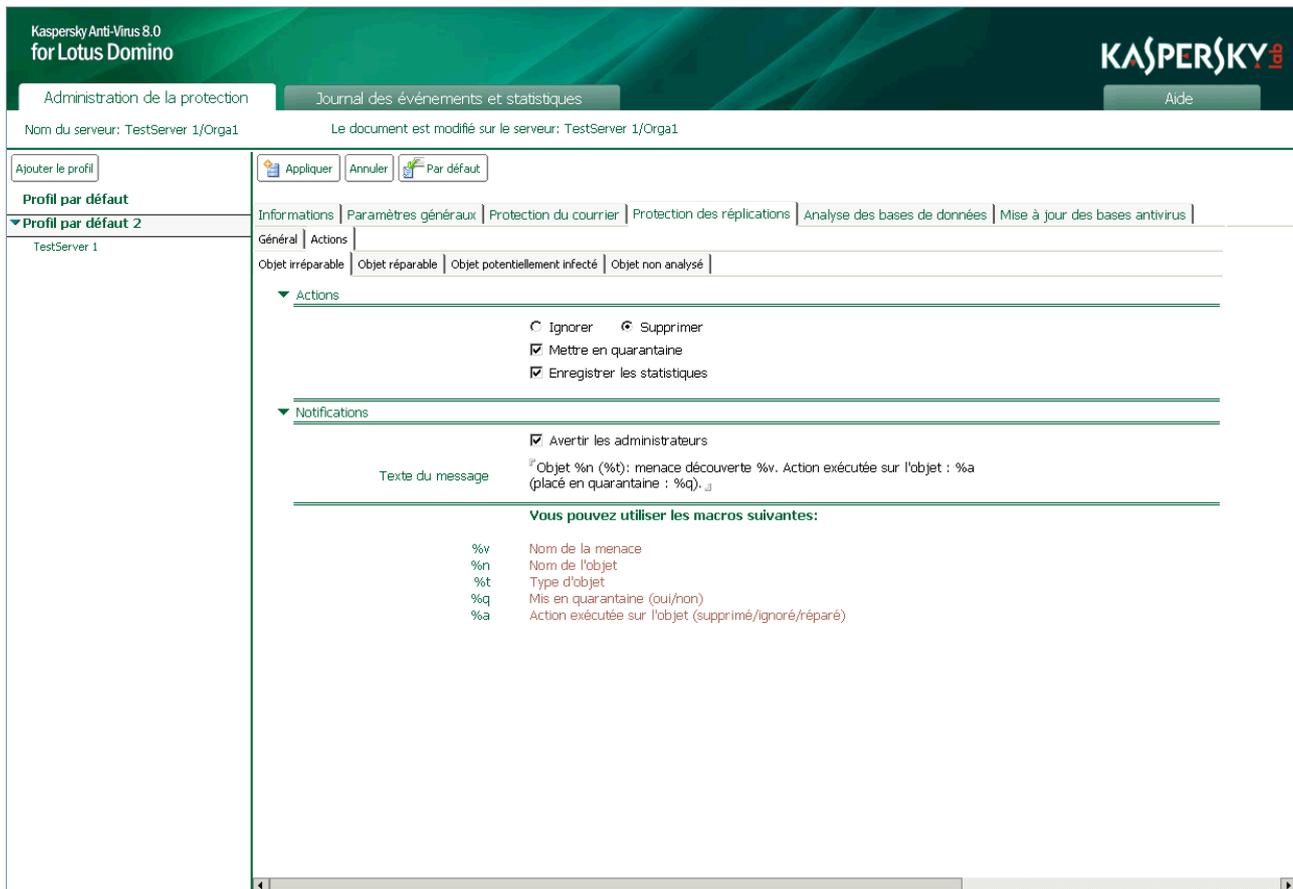


Illustration 24 : Configuration des actions à exécuter sur les objets irréparables dans le cadre de la protection des répliquions

4. Sous l'onglet **Actions**, sélectionnez l'onglet correspondant à l'état de l'objet dont vous souhaitez configurer les paramètres de traitement. Vous avez le choix parmi les onglets suivants :
 - **Objet irréparable** : configuration des paramètres de traitement des objets irréparables.
 - **Objet réparable** : configuration des paramètres de traitement des objets réparables.
 - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
 - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.
5. Dans le groupe **Actions** (cf. ill. ci-dessus), sélectionnez l'action à exécuter sur l'objet détecté et, le cas échéant, cochez les cases suivantes :
 - **Mettre en quarantaine** : avant le traitement, une copie de l'objet sera placée dans la base de données Quarantaine.

Seul l'objet est placé en quarantaine. Le document auquel il appartient n'est pas mis en quarantaine.

- **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées dans les sources définies par le champ **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs sources de conservation des informations sont sélectionnées simultanément, l'écriture sera réalisée simultanément dans les lieux de stockage des informations indiqués.

- **Sur la console** (journal système Domino log.nsf) ;
 - **Dans le journal** ;
 - **Dans le fichier** (nom du fichier par défaut server.log).
6. Dans le groupe **Notifications** (cf. ill. ci-dessus), configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. rubrique " Notifications " à la page [106](#)).
 7. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

FILTRAGE DES PIÈCES JOINTES EN MODE DE PROTECTION DES RÉPLICATIONS

Kaspersky Anti-Virus peut filtrer les objets joints aux documents (cf. rubrique " Algorithme de filtrage des pièces jointes " à la page [23](#)). 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 n'est pas activé par défaut dans la protection des répliques.

➡ *Pour configurer le filtrage des pièces jointes, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection des répliquions**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

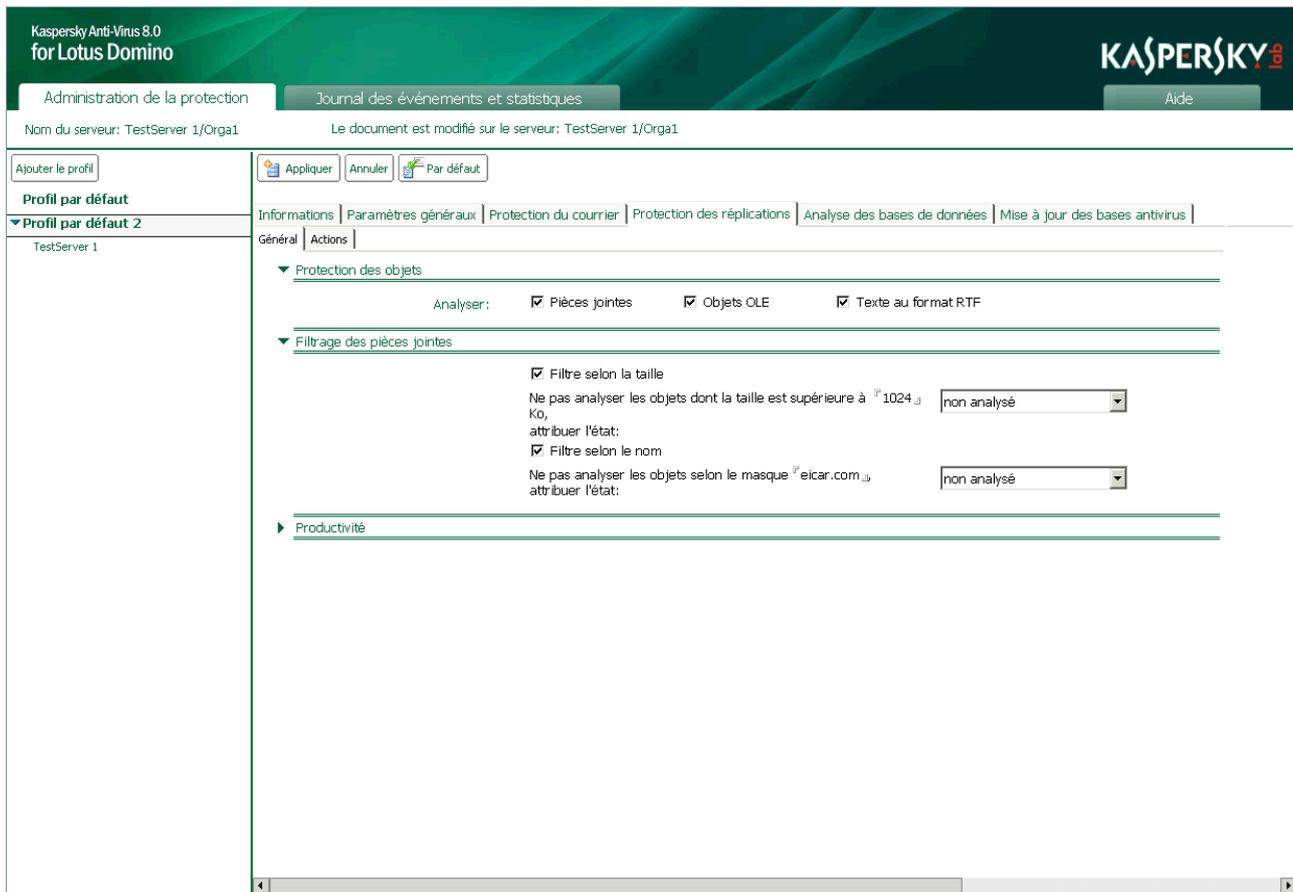


Illustration 25 : Sélection des objets de la protection des répliquions

4. Dans le groupe **Filtrage des pièces jointes** (cf. ill. ci-dessus), cochez les cases suivantes et définissez les paramètres correspondants si vous souhaitez filtrer les objets :
- **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 est supérieure à**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera filtré et exclu de l'analyse antivirus. Dans la liste déroulante, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus.
 - **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 filtrés et exclus de l'analyse antivirus. Dans la liste déroulante, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus.

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

Vous pouvez désigner plusieurs masques et les séparer par " ; ". Pour composer les masques, utilisez les caractères : * et ? (cf. rubrique " Filtrage des pièces jointes du courrier " à la page [64](#)).

Si la case n'est pas cochée, le filtrage des objets correspondant n'aura pas lieu.

5. 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 DONNÉES

L'analyse des bases de données est lancée selon la programmation ou à la demande de l'utilisateur. Les paramètres de l'analyse sont définis via un profil ; il n'est pas possible de définir des paramètres individuels pour le serveur. L'activation ou la désactivation de l'analyse des bases de données (cf. rubrique " Activation et désactivation de l'analyse des bases de données " à la page [77](#)) est possible uniquement pour chaque serveur séparément.

Après l'installation de l'application, ce sont les valeurs par défaut qui sont utilisées (cf. rubrique " Protection du serveur par défaut " à la page [47](#)). Vous pouvez les modifier en fonction des exigences de sécurité du serveur Domino protégé. Une partie des paramètres cités ici est désactivée par défaut ou peut être désactivée par l'administrateur.

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 Domino) et dans tous ses sous-répertoires. Vous pouvez activer ou désactiver l'analyse des bases de données situées dans les sous-répertoires du répertoire data jusqu'au niveau le plus bas de la hiérarchie.

Kaspersky Anti-Virus permet d'exclure certaines bases de données de l'analyse. La base de données Quarantaine est exclue de l'analyse par défaut (kavquarantine.nsf).

De plus, vous pouvez définir les masques des noms des fichiers de bases de données à analyser (cf. rubrique " Sélection des objets à analyser des bases de données " à la page [78](#)). Dans ce cas, Kaspersky Anti-Virus analysera uniquement les fichiers des bases de données définis à l'aide des masques.

Par défaut les champs des documents des bases de données au format Rich Text, les objets joints au document et les objets OLE intégrés sont soumis à la recherche de menaces.

Le cas échéant, vous pouvez désactiver l'analyse des pièces jointes, des objets OLE et du contenu des champs au format Rich Text (cf. rubrique " Sélection des objets à analyser des bases de données " à la page [78](#)). Vous pouvez également limiter la durée d'analyse d'un objet afin d'accélérer la vitesse globale d'analyse des répliqués (cf. rubrique " Productivité " à la page [86](#)).

Les objets infectés, potentiellement infectés et non analysés suite à un échec ou en raison de dégâts découverts suite à l'analyse sont traités conformément aux paramètres d'analyse des bases de données (cf. rubrique " Actions à exécuter sur les objets en mode d'analyse des bases de données " à la page [80](#)).

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. rubrique " Filtrage des pièces jointes en mode d'analyse des bases de données " à la page [82](#)).

Avant le traitement de l'objet une copie est placée par défaut en quarantaine (cf. page [88](#)).

La notification sur l'analyse du document par Kaspersky Anti-Virus et la description des actions exécutées sont envoyées aux administrateurs (cf. rubrique " Notifications " à la page [106](#)). Les informations relatives aux résultats de l'analyse et aux actions exécutées sont consignées dans la base de données Journal des événements et statistiques.

DANS CETTE SECTION

Activation et désactivation de l'analyse des bases de données	77
Sélection des objets à analyser des bases de données	78
Actions à exécuter sur les objets en mode d'analyse des bases de données	80
Filtrage des pièces jointes en mode d'analyse des bases de données	82
Analyse selon la programmation	84
Analyse manuelle	85

ACTIVATION ET DÉSACTIVATION DE L'ANALYSE DES BASES DE DONNÉES

L'analyse des bases de données est activée par défaut et ce composant de la protection est lancé automatiquement au démarrage du serveur Domino. 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/désactiver l'analyse des bases de données, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous souhaitez activer/désactiver l'analyse des bases de données.

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

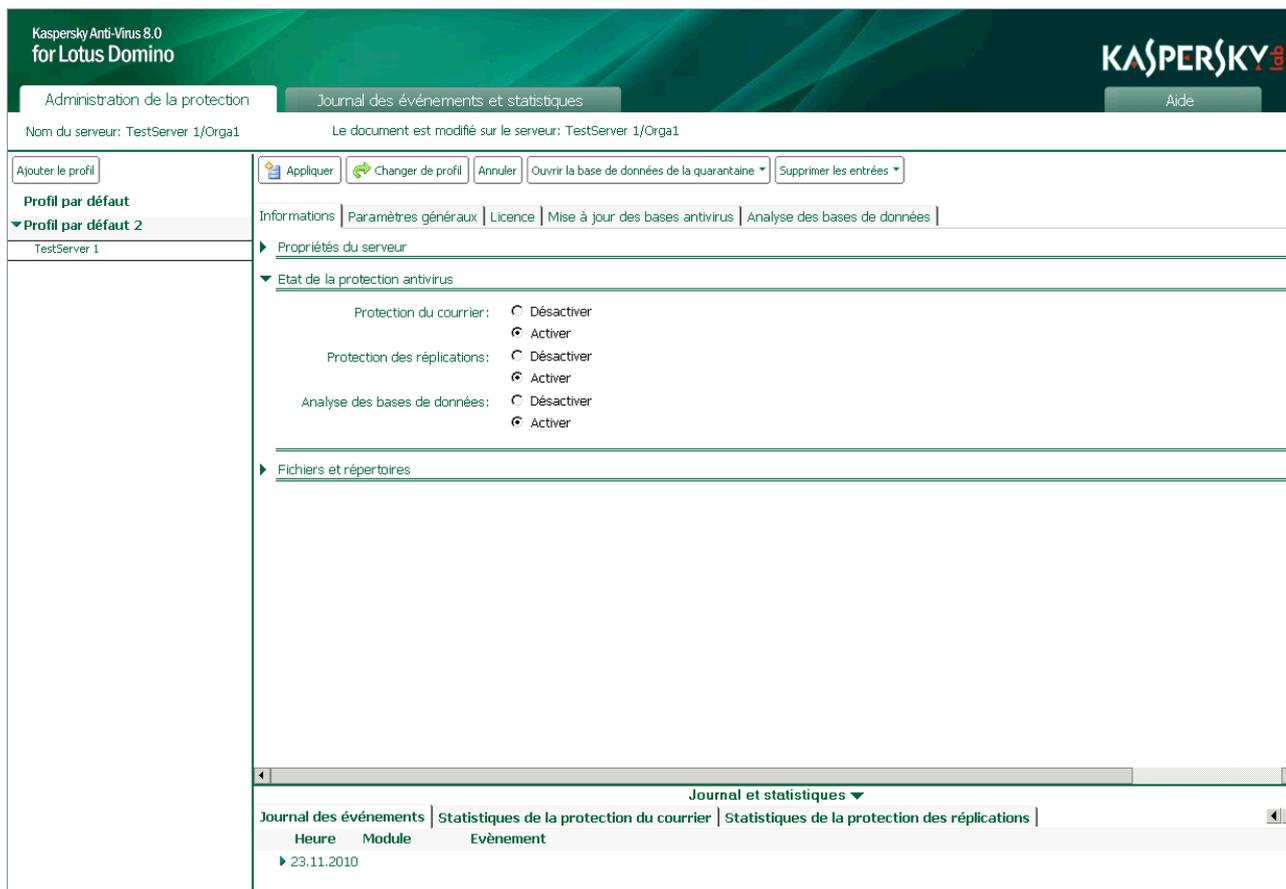


Illustration 26: Activation/désactivation de l'analyse des bases de données

- Dans le groupe **Etat de la protection antivirus**, sur la ligne **Analyse des bases de données** (cf. ill. ci-dessus), choisissez l'option voulue : **Activer** ou **Désactiver**.
- Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

SÉLECTION DES OBJETS À ANALYSER DES BASES DE DONNÉES

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

➤ Pour sélectionner les objets pour l'analyse antivirus, procédez comme suit :

- Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.

2. Dans le volet de navigation, sélectionnez le profil dont vous souhaitez modifier les paramètres.
3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Analyse des bases de données**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

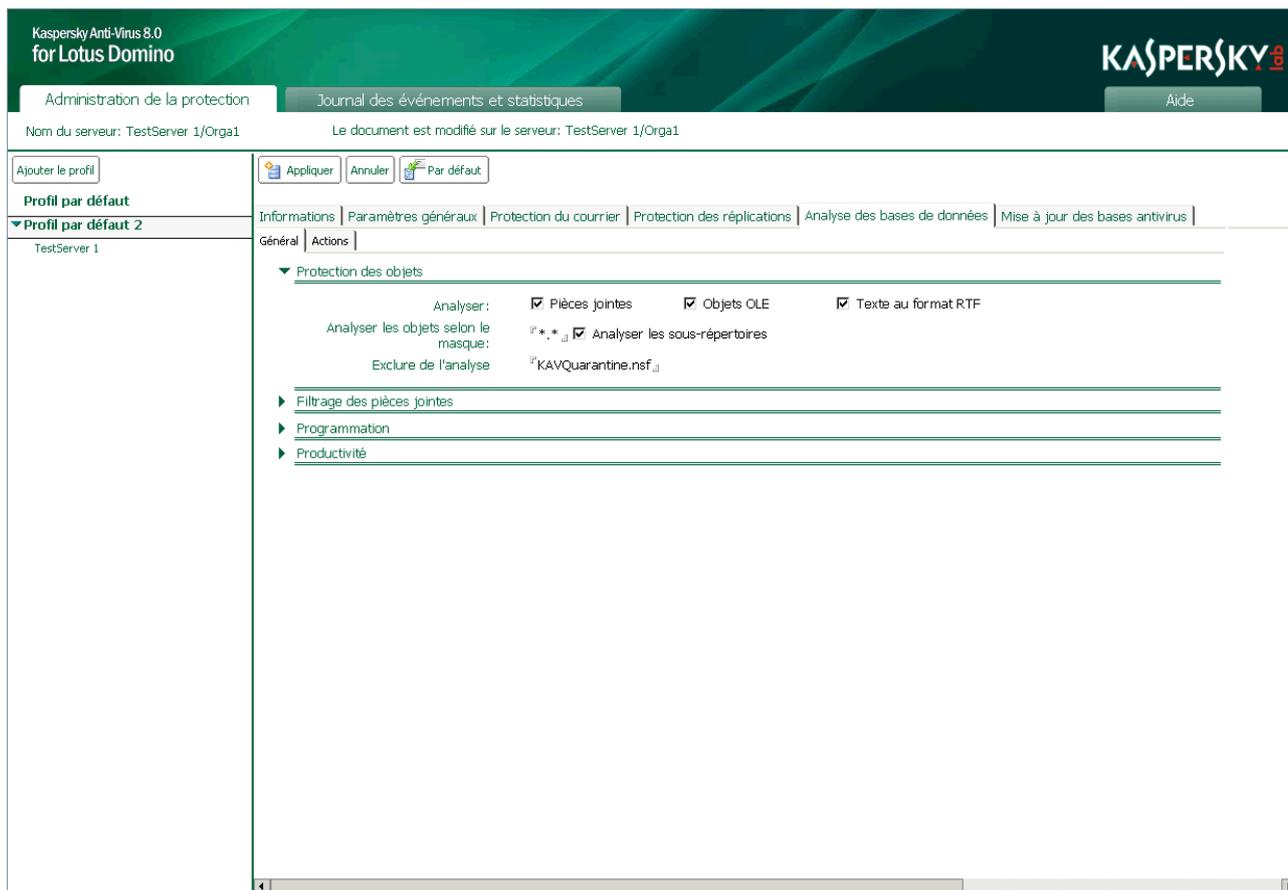


Illustration 27: Sélection des objets à analyser des bases de données

4. Dans le groupe **Protection des objets**, cochez les cases suivantes pour pouvoir analyser les objets :
 - **Pièces jointes** : analyser tout fichier joint au document.
 - **Objets OLE** : analyser tous les objets OLE intégrés au document.
 - **Texte au format RTF** : analyser les champs du document au format Rich Text.

Si la case n'est pas cochée, l'analyse des objets correspondant n'aura pas lieu.

5. 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. Les caractères * et ? peuvent être utilisés dans la composition des masques.
6. Cochez la case **Analyser les sous-répertoires** pour que Kaspersky Anti-Virus analyse les bases de données situées 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 bases de données situées dans le répertoire racine data, décochez la case.

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

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

ACTIONS À EXÉCUTER SUR LES OBJETS EN MODE 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. rubrique " Traitement des objets et actions exécutées sur ceux-ci " à la page [24](#)). Les objets sains sont ignorés sans aucune modification. Les actions à exécuter sur les objets réparables, irréparables, potentiellement infectés et non analysés sont définies par l'administrateur. Les actions qui seront exécutées par l'application sont définies pour chaque état individuel.

Les actions suivantes sont exécutées par défaut sur les objets :

- Si l'objet est considéré comme réparable, Kaspersky Anti-Virus le répare. L'objet réparé est conservé dans le document à l'adresse d'origine. Si la réparation de l'objet a échoué, Kaspersky Anti-Virus le supprime du document.

Peu importe la configuration des paramètres, la réparation des objet OLE s'effectue uniquement à l'aide d'une suppression.

- Si l'objet est considéré comme irréparable, Kaspersky Anti-Virus le supprime du document.
- 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 prévu pour l'analyse s'est écoulé), Kaspersky Anti-Virus supprime l'objet du document.

Par défaut, une copie de l'objet est conservée dans la base de données Quarantaine (cf. page [88](#)) avant le traitement. Les informations sur les objets découverts et les actions exécutées peuvent être envoyées aux administrateurs (cf. rubrique " Notifications " à la page [106](#)) et conservées dans la base de données Journal des événements et statistiques (cf. rubrique " Journal des événements et statistiques " à la page [95](#)).

Les actions qui seront exécutées par l'application sont définies dans les paramètres d'analyse des bases de données pour chaque état séparément.

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

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

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

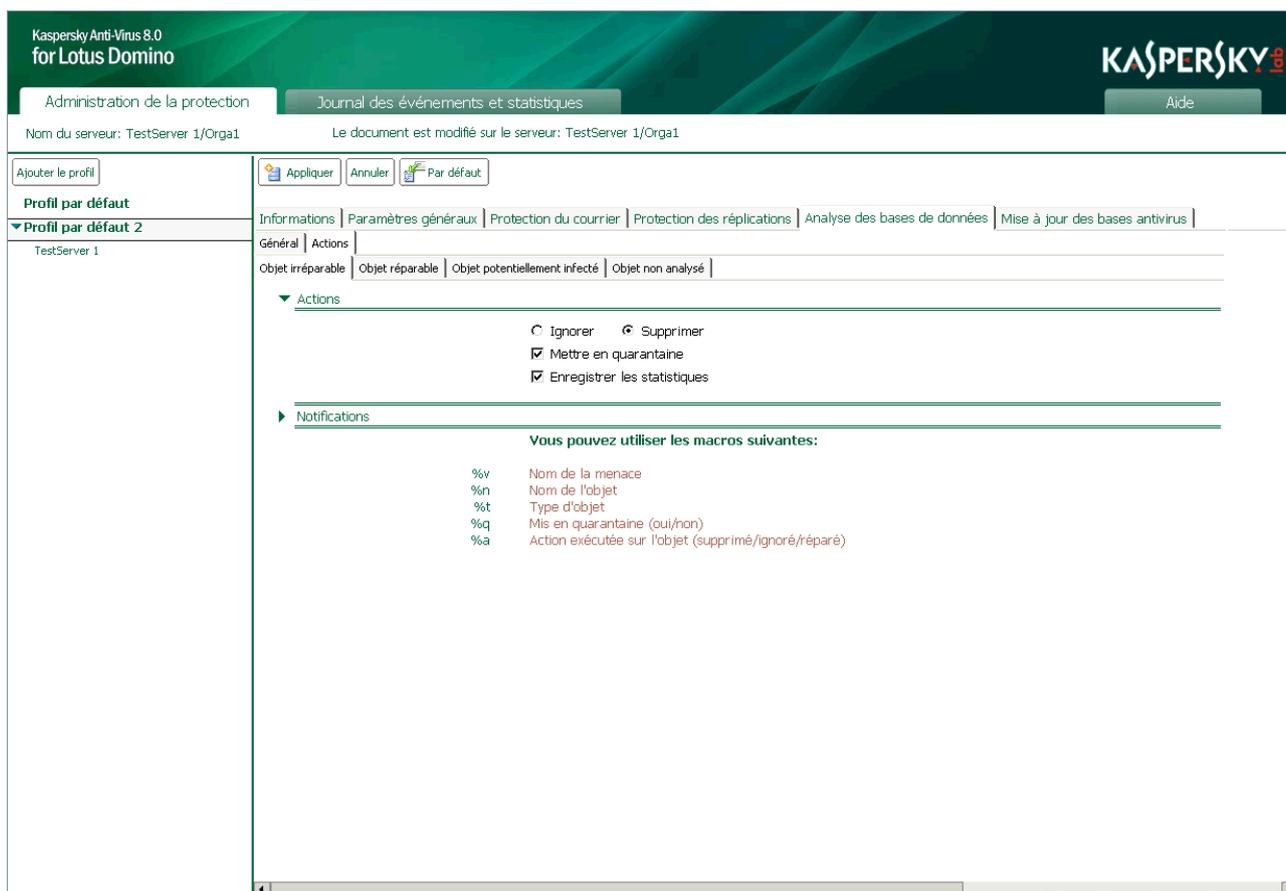


Illustration 28 : Configuration des actions à exécuter sur les objets irréparables en mode d'analyse des bases de données

4. Sous l'onglet **Actions**, sélectionnez l'onglet correspondant à l'état de l'objet dont vous souhaitez configurer les paramètres de traitement. Vous avez le choix parmi les onglets suivants :
 - **Objet irréparable** : configuration des paramètres de traitement des objets irréparables.
 - **Objet réparable** : configuration des paramètres de traitement des objets réparables.
 - **Objet potentiellement infecté** : configuration des paramètres de traitement des objets potentiellement infectés.
 - **Objet non analysé** : configuration des paramètres de traitement des objets non analysés.
5. Dans le groupe **Actions** (cf. ill. ci-dessus), sélectionnez l'action à exécuter sur l'objet détecté et, le cas échéant, cochez les cases suivantes :
 - **Mettre en quarantaine** : avant le traitement, une copie de l'objet sera placée dans la base de données Quarantaine.

Seul l'objet est placé en quarantaine. Le document auquel il appartient n'est pas mis en quarantaine.

- **Enregistrer les statistiques** : les informations relatives à l'objet détecté et aux actions exécutées sont consignées dans les sources définies par le champ **Enregistrer les informations**, sous l'onglet **Paramètres généraux**. Si plusieurs sources de conservation des informations sont sélectionnées simultanément, l'écriture sera réalisée simultanément dans les lieux de stockage des informations indiqués.

- **Sur la console** (journal système Domino log.nsf) ;
 - **Dans le journal** ;
 - **Dans le fichier** (nom du fichier par défaut server.log).
6. Dans le groupe **Notifications** (cf. ill. ci-dessus), configurez les paramètres selon lesquels les notifications relatives à l'objet découvert et aux actions exécutées seront envoyées (cf. rubrique " Notifications " à la page [106](#)).
 7. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

FILTRAGE DES PIÈCES JOINTES EN MODE D'ANALYSE DES BASES DE DONNÉES

Pendant l'analyse des bases de données, Kaspersky Anti-Virus permet d'exclure de l'analyse antivirus les pièces jointes qui répondent aux paramètres de filtrage. 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 en mode de protection du courrier. Le filtrage des pièces jointes n'est pas activé par défaut dans l'analyse des bases de données.

Par défaut, les objets filtrés reçoivent l'état *non analysé* et ils sont soumis aux actions définies pour cette catégorie d'objet dans les paramètres de l'analyse des bases de données.

► *Pour configurer le filtrage des pièces jointes, 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 modifier les paramètres.

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

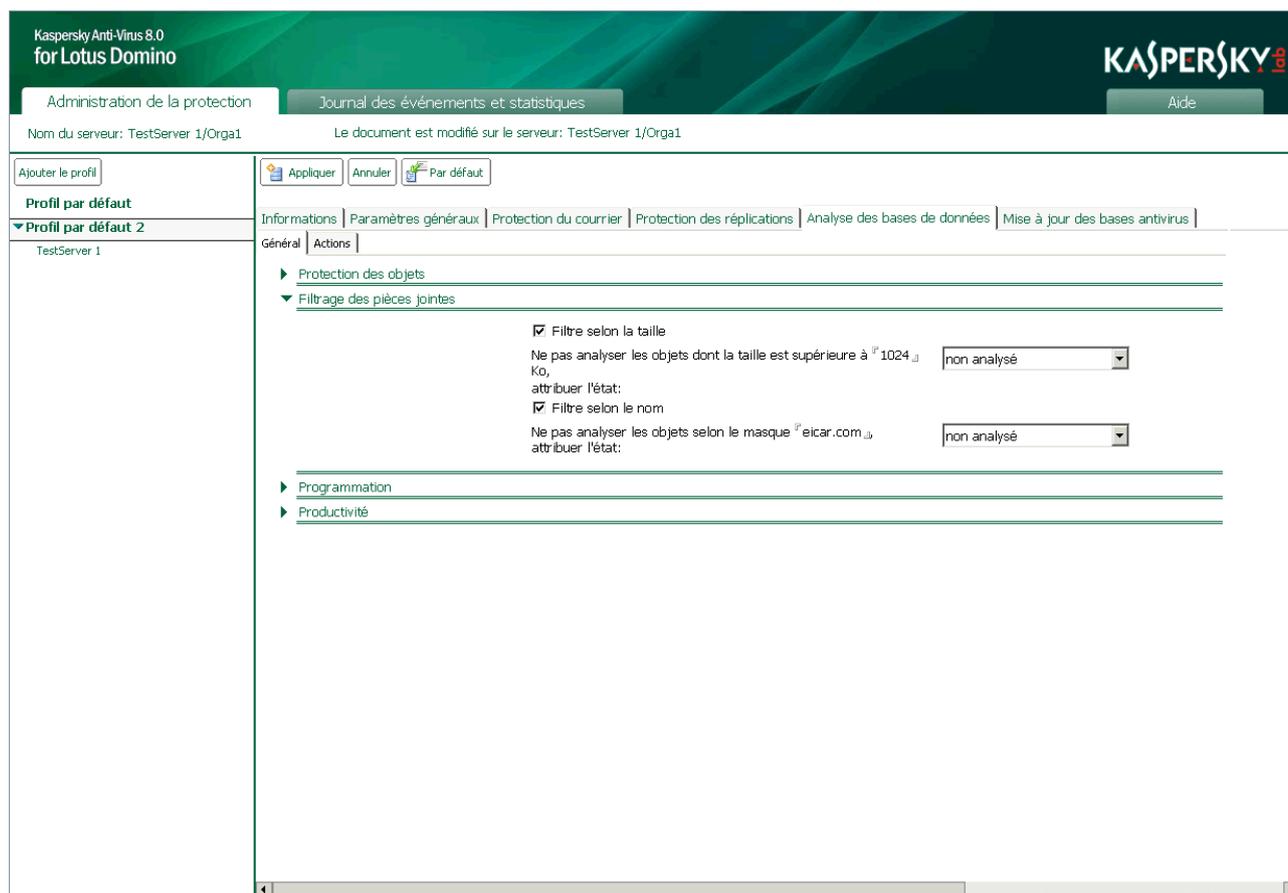


Illustration 29 : Configuration du filtrage des pièces jointes en mode d'analyse des bases de données

4. Dans le groupe **Filtrage des pièces jointes** (cf. ill. ci-dessus), cochez les cases suivantes et définissez les paramètres correspondants si vous souhaitez filtrer les objets :
 - **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 est supérieure à**, définissez la valeur maximale, en Ko, au-delà de laquelle l'objet sera filtré et exclu de l'analyse antivirus. Dans la liste déroulante, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus.
 - **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 filtrés et exclus de l'analyse antivirus. Dans la liste déroulante, choisissez l'état selon lequel l'objet sera traité par Kaspersky Anti-Virus.

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

Vous pouvez désigner plusieurs masques et les séparer par " ; ". Pour composer les masques, utilisez les caractères : * et ? (cf. rubrique " Filtrage des pièces jointes du courrier " à la page [64](#)).

Si la case n'est pas cochée, le filtrage des objets correspondant n'aura pas lieu.

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

ANALYSE SELON LA PROGRAMMATION

Kaspersky Anti-Virus analyse les bases de données conformément à la programmation de l'analyse. Vous pouvez programmer l'analyse uniquement pour un groupe de serveurs via un profil.

➔ Pour configurer la programmation de l'analyse, 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 modifier les paramètres.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et dans la zone d'administration, sélectionnez l'onglet **Analyse des bases de données** (cf. ill. ci-après).

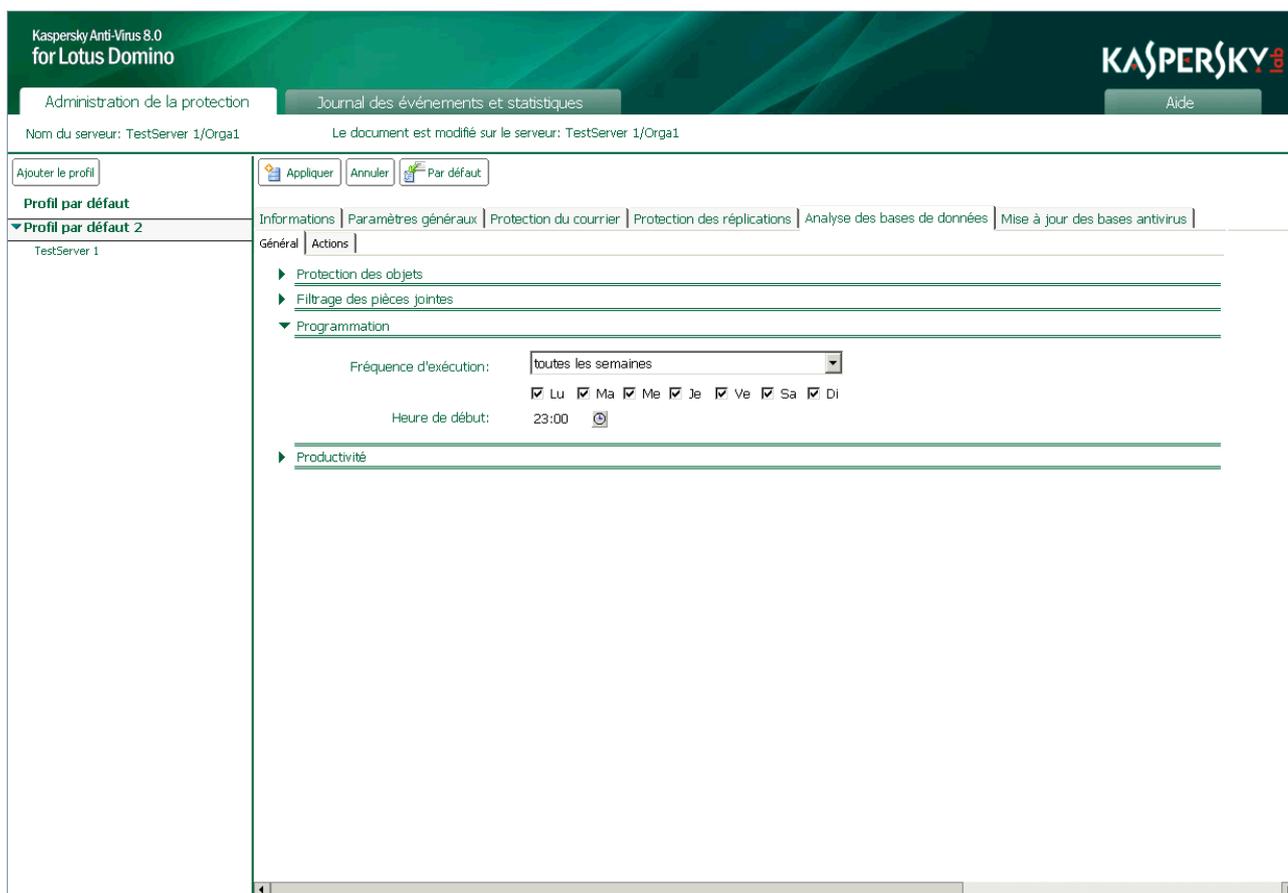


Illustration 30 : Configuration de la planification de l'analyse des bases de données

4. Dans le groupe **Programmation** (cf. ill. ci-dessus) choisissez une des options suivantes dans la liste déroulante **Fréquence d'exécution** :
 - **toutes les semaines** : l'analyse des bases de données aura lieu chaque semaine, le jour défini et à l'heure reprise dans le champ **Heure de début**. Cochez la case en regard des jours où l'analyse des bases de données sera lancée et saisissez l'heure souhaitée dans le champ **Heure de début**. Le format doit être - **hh:mm**.
 - **tous les mois** : l'analyse des bases de données aura lieu une fois par mois, le jour indiqué et à l'heure reprise dans le champ **Heure de début**. Saisissez l'heure souhaitée dans le champ **Heure de début**. Le format doit être - **hh:mm**.
5. 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

Le lancement manuel de l'analyse des bases de données est possible pour un serveur uniquement ; ce mode de lancement n'est pas prévu pour un groupe de serveurs. L'analyse peut être lancée manuellement même si l'analyse programmée est désactivée.

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous voulez lancer l'analyse.
3. Dans la zone d'administration, sélectionnez l'onglet **Analyse des bases de données** (cf. ill. ci-après). 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.

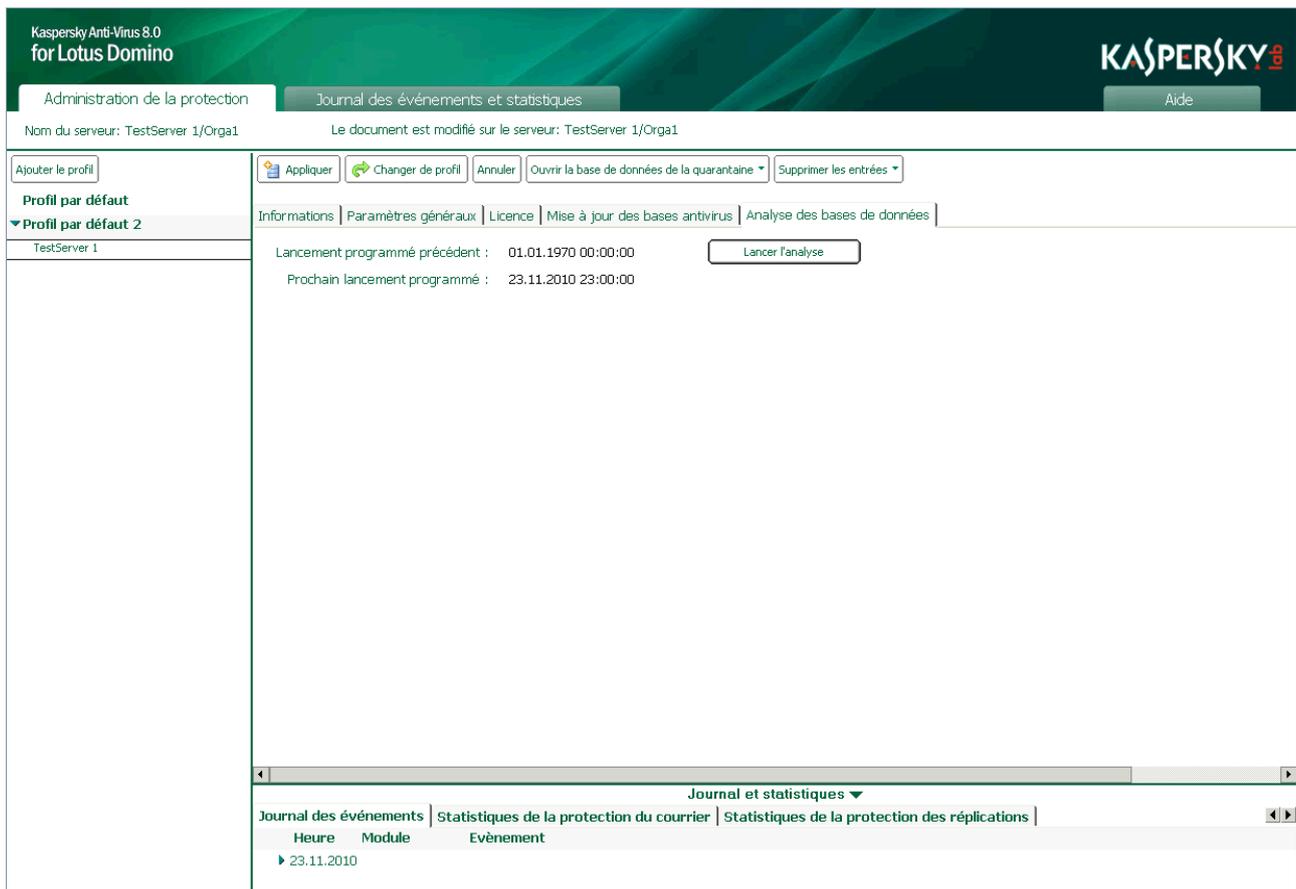


Illustration 31 : Lancement manuel de l'analyse des bases de données

4. Cliquez sur **Lancer l'analyser** afin de lancer l'analyse des bases de données.

L'analyse des bases de données peut également être lancée depuis la ligne de commande (cf. rubrique " Utilisation via la console du serveur " à la page [119](#)).

PRODUCTIVITÉ

Kaspersky Anti-Virus permet de régler les performances de l'application lors de l'analyse d'objets à l'aide des paramètres suivants :

- *Durée d'analyse d'un objet.* Si l'analyse dure plus que la valeur définie, elle est suspendue et l'objet reçoit l'état *non analysé* et l'application passe à l'analyse de l'objet suivant.
- *Analyse d'un objet dans la mémoire.* 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.

Vous pouvez configurer les paramètres de productivité de l'analyse. Pour chaque composant de la protection, les paramètres des performances de l'analyse sont définis séparément.

➔ *Pour configurer les paramètres des performances de l'analyse, 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 modifier les paramètres.
3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier/Protection des réplifications/Analyse des bases de données**, sélectionnez l'onglet **Général** (cf. ill. ci-après).

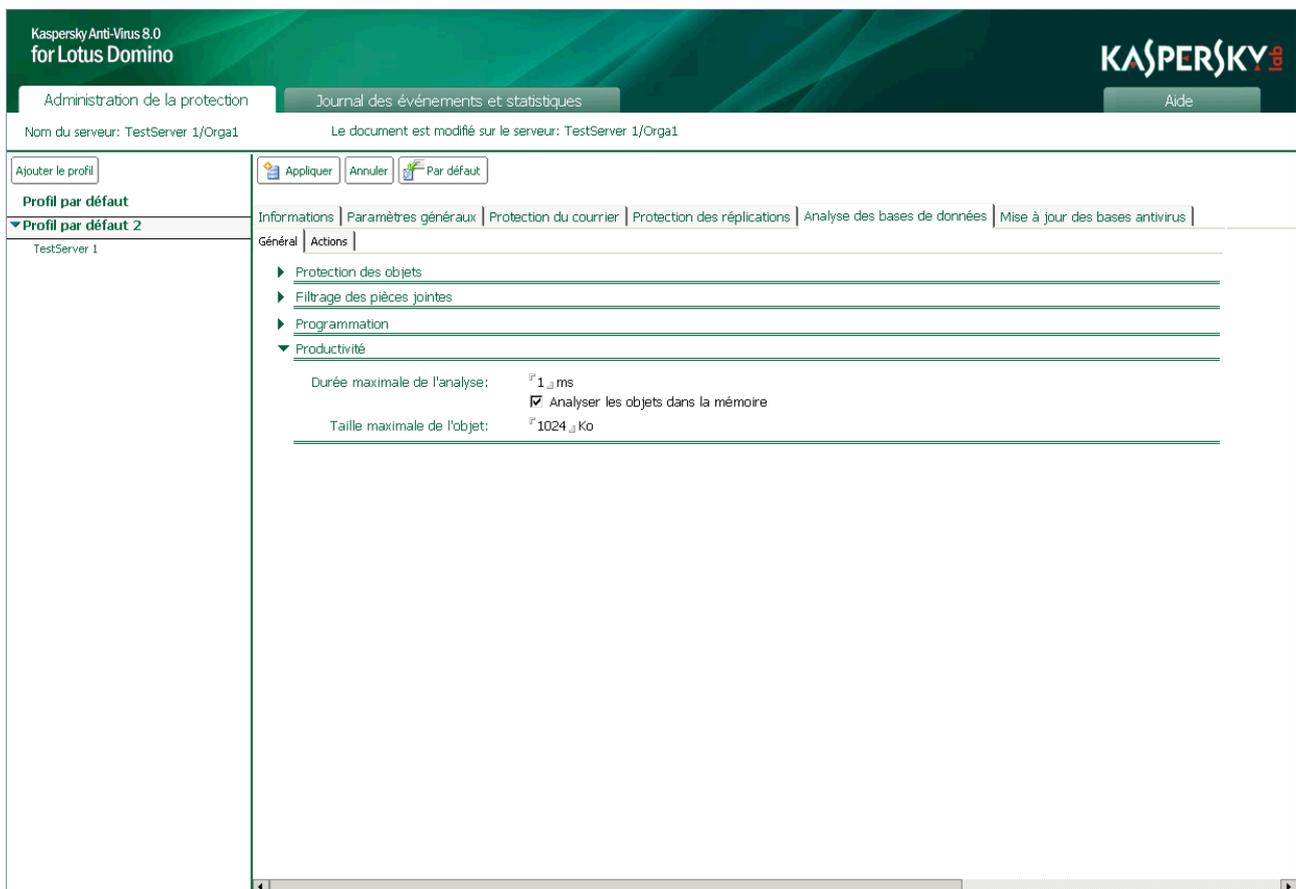


Illustration 32 : Configuration des paramètres de productivité de l'analyse des bases de données

4. Dans le groupe **Productivité**, configurez les paramètres selon lesquels l'analyse sera réalisée. 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 300 ms.
 - 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

Selon les paramètres de la protection du courrier, de la protection des répliques ou de l'analyse des bases de données, les copies des objets isolés suite au filtrage ou à l'analyse antivirus sont placés 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 antivirus de ce serveur. Lors de l'installation de l'application, vous pouvez décider d'enregistrer les objets de la quarantaine dans toutes les répliques ou de conserver uniquement les objets de son serveur.

Par défaut, les objets mis en quarantaine sont les objets considérés comme irréparables, réparables, potentiellement infectés et non analysés à l'issue de l'analyse antivirus. Les catégories exactes d'objets mis en quarantaine sont définies dans les paramètres de la protection du courrier, de la protection des répliques et de l'analyse des bases de données pour chaque catégorie d'objets séparément.

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

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. rubrique " Interface de l'application " à la page [36](#)).

Pour une recherche et un affichage plus convivial des informations relatives aux objets mis en quarantaine suite à l'analyse des messages électroniques, des répliques et des bases de données, il existe plusieurs rubriques (cf. rubrique " Consultation des objets placés en quarantaine " à la page [88](#)).

Par défaut, la durée maximale de conservation des objets en quarantaine est de 30 jours. Vous pouvez modifier la durée de conservation des objets en quarantaine dans les paramètres du serveur (cf. rubrique " Configuration des paramètres de la quarantaine " à la page [93](#)). Si la durée de conservation des objets (cf. rubrique " Configuration des paramètres de la quarantaine " à la page [93](#)) est limitée, à l'issue de celle-ci, les objets dont la durée de conservation a atteint la limite seront supprimés de la base de données. 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 avoir 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 mis antérieurement en quarantaine (cf. rubrique " Actions à exécuter sur les objets placés en quarantaine " à la page [91](#)) ou de modifier les paramètres de conservation des objets mis en quarantaine afin de la purger.

DANS CETTE SECTION

Consultation des objets placés en quarantaine	88
Actions à exécuter sur les objets placés en quarantaine.....	91
Configuration de la quarantaine	93

CONSULTATION DES OBJETS PLACÉS EN QUARANTAINE

La consultation des objets placés en quarantaine s'opère via l'interface utilisateur de la base de données Centre d'administration. Les objets mis en quarantaine à l'issue de l'analyse des messages électroniques, des répliques et des bases de données sont repris dans des rubriques distinctes.

Vous pouvez consulter les types d'objets suivants placés en quarantaine : messages, bases de données, répliquions. Chaque type d'objet apparaît dans une nouvelle fenêtre. Vous pouvez ouvrir les entrées de la quarantaine directement pour tous les serveurs en une fois.

➔ Pour consulter les objets mis en quarantaine et les informations à leur sujet, procédez comme suit :

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un serveur au hasard dans n'importe quel profil.

Si la case **Conserver les objets de la quarantaine dans toutes les répliquions** n'avait pas été cochée lors de l'installation dans les paramètres de déploiement, chaque réplique conservera uniquement les entrées d'un serveur (actuel).

3. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données de la quarantaine** et dans la liste déroulante qui s'ouvre, sélectionnez une des options suivantes :

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

Cette action entraînera l'affichage des entrées de la quarantaine pour tous les serveurs dans la zone d'administration (cf. ill. ci-après). Les entrées relatives aux messages électroniques mis en quarantaine sont regroupées par date et par adresse électronique de l'expéditeur des messages. Les entrées relatives aux objets mis en quarantaine suite à l'analyse des bases de données et des répliquions sont regroupées par date de mise en quarantaine des objets et par nom des bases de données auxquelles appartiennent les documents analysés.

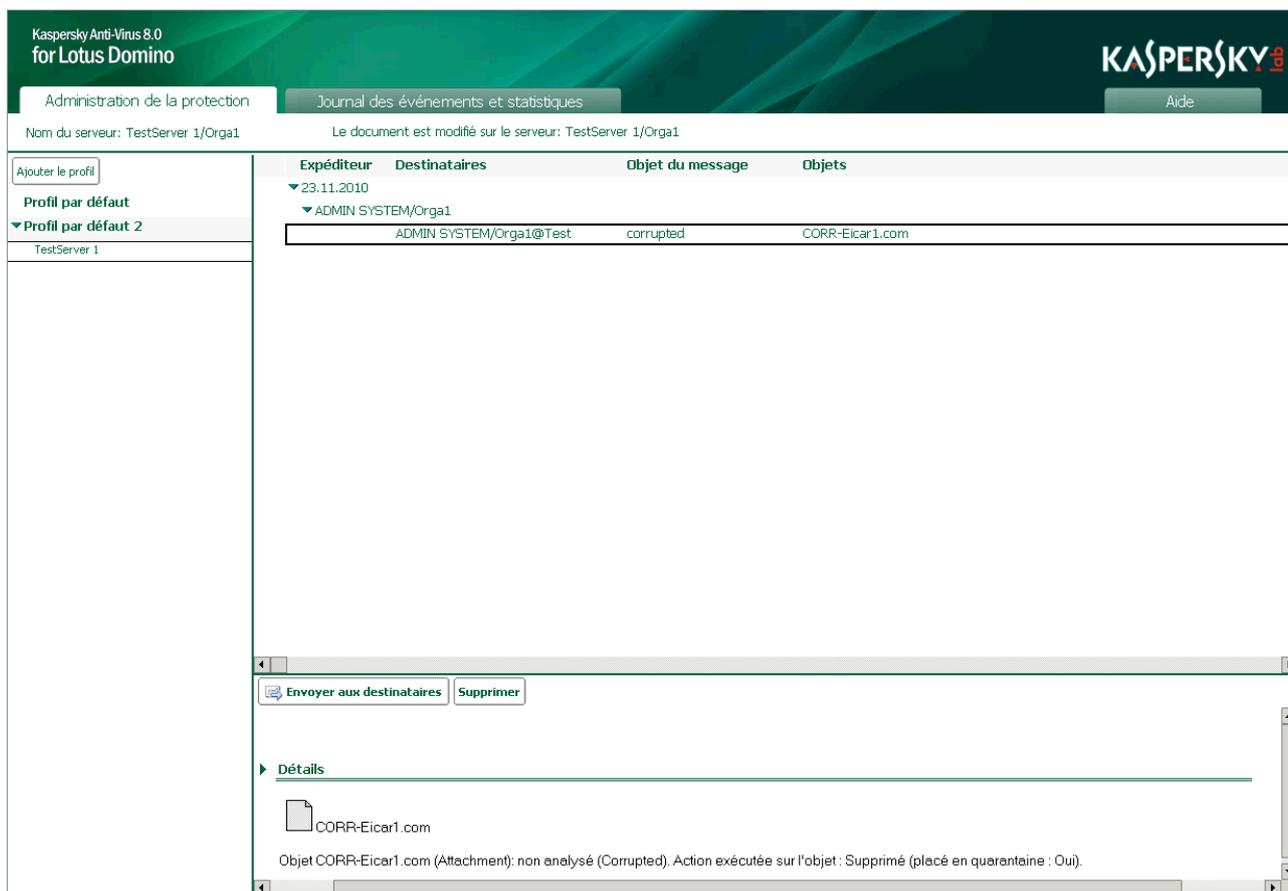


Illustration 33 : Consultation des objets placés en quarantaine

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

Vous pouvez également consulter des informations complémentaires sur chacun des objets mis en quarantaine.

Pour ce faire, dans la liste des entrées, sélectionnez avec la souris l'objet dont vous souhaitez consulter les informations. Cette action entraîne l'affichage dans le groupe **Détails** des 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 d'une copie du message électronique.
 - **Copie cachée** : adresses électroniques des destinataires d'une copie cachée du message électronique.
 - **Objet du message** : objet du message dans lequel la menace a été découverte.
 - Liste des fichiers joints.
 - Informations textuelles contenant le nom de l'objet, le nom de la menace détectée et la liste des actions exécutées sur l'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 le nom du serveur sur lequel ces modifications ont été introduites, format de l'entrée : **Nom de l'utilisateur/nom du serveur**.
 - **Document** : numéro (nom) du document sur le serveur Domino dans lequel la menace a été découverte.
 - Liste des fichiers joints.
 - Informations textuelles contenant le nom de l'objet, le nom de la menace détectée et la liste des actions exécutées sur l'objet.

ACTIONS À EXÉCUTER SUR LES OBJETS PLACÉS EN QUARANTAINE

Vous pouvez exécuter les actions suivantes sur les objets mis en quarantaine :

- Supprimer les objets manuellement ;
- Supprimer les entrées plus anciennes que le nombre de jours indiqués ;
- Transmettre les messages électroniques aux destinataires.

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

➡ *Pour supprimer un objet de la quarantaine, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un serveur au hasard dans n'importe quel profil.
3. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données de la quarantaine** et dans la liste déroulante qui s'ouvre, sélectionnez une des options suivantes :
 - **Messages électroniques.**
 - **Bases de données.**
 - **Répliquions.**

Cette action entraînera l'affichage des entrées de la quarantaine pour tous les serveurs dans la zone d'administration.

4. Pour déployer la liste des entrées regroupées, cliquez sur le bouton ▶.

5. Dans la liste des entrées, sélectionnez avec la souris l'objet que vous voulez supprimer de la quarantaine, puis dans la zone de consultation, cliquez sur le bouton **Supprimer** (cf. ill. ci-après).

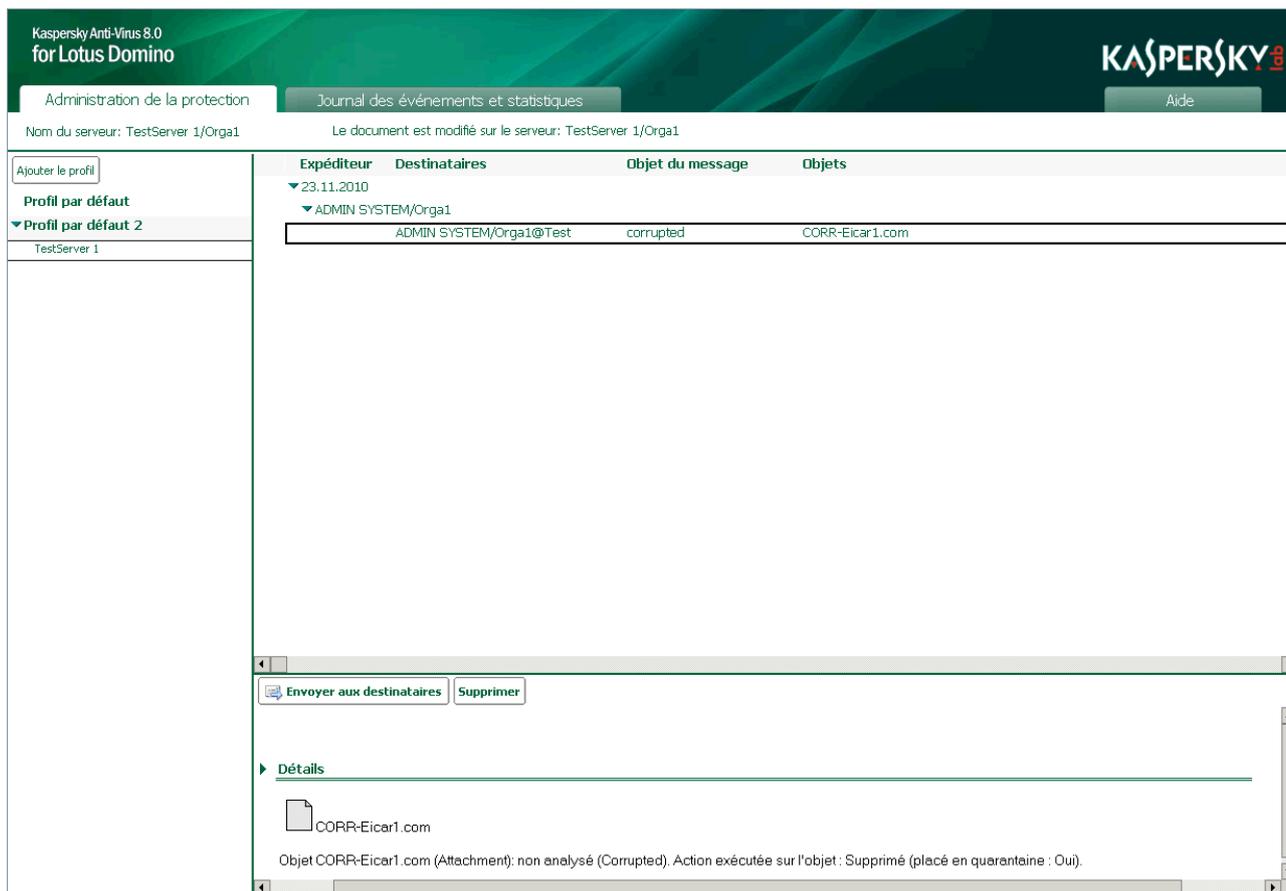


Illustration 34 : Suppression des objets de la quarantaine

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

- Pour transférer un message électronique de la quarantaine aux destinataires, procédez comme suit :
 1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
 2. Dans le volet de navigation, sélectionnez un serveur au hasard dans n'importe quel profil.
 3. Dans le volet des actions, cliquez sur le bouton **Ouvrir la base de données de la quarantaine** et dans la liste déroulante qui s'ouvre, sélectionnez la valeur **Messages électroniques**.

Suite à cette action, les entrées des messages mis en quarantaine sur tous les serveurs apparaissent dans la zone d'administration.

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

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

- Pour supprimer les entrées de la quarantaine conservées plus longtemps que le nombre de jours maximum défini, procédez comme suit :

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.

2. Dans le volet de navigation, sélectionnez un serveur au hasard dans n'importe quel profil.
3. Dans le volet des actions, cliquez sur le bouton **Supprimer les entrées** et dans la liste déroulante, choisissez la valeur **Quarantaine**.
4. Dans la fenêtre qui s'ouvre, saisissez le nombre de jours de conservation maximum au delà duquel les entrées seront supprimées de la quarantaine, puis cliquez sur **OK**.

Cette action entraînera la suppression des entrées de la base de données Quarantaine dont la durée de conservation est supérieure au nombre de jours indiqués.

CONFIGURATION DE LA QUARANTAINE

Vous pouvez modifier la durée de conservation des objets en quarantaine dans les paramètres du serveur.

➔ Pour modifier la durée de conservation des objets en quarantaine, procédez comme suit :

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur dont vous souhaitez modifier les paramètres.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-après).

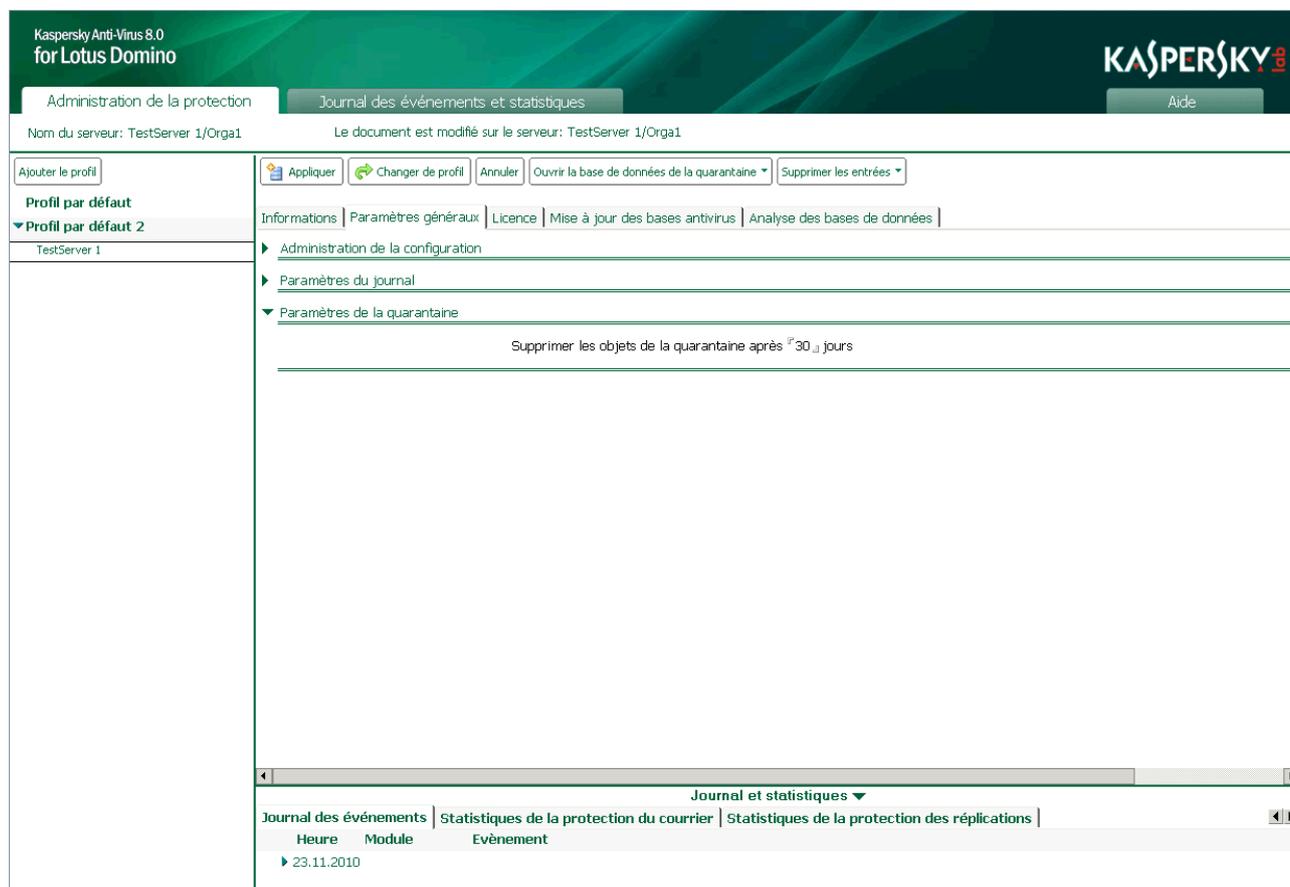


Illustration 35 : Configuration de la quarantaine

4. Dans le groupe **Paramètres de la quarantaine**, indiquez la durée de conservation, en jours, des objets mis en quarantaine. La durée de conservation par défaut des objets est de 30 jours.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

Dans les paramètres de la protection du courrier, des répliques et des bases de données, vous pouvez définir les catégories d'objets à mettre en quarantaine. La configuration des paramètres s'opère pour chaque catégorie d'objets séparément.

De plus, si vous souhaitez qu'à l'issue de l'analyse antivirus le message électronique entier soit mis en quarantaine et non pas seulement ses objets, dans les paramètres de la protection, sous l'onglet **Avancé**, cochez la case **Mettre le message complet en quarantaine** (cf. rubrique " Actions à exécuter sur les objets du courrier " à la page [60](#)).

JOURNAL DES ÉVÉNEMENTS 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.

La base de données Journal des événements et statistiques sert à conserver 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 l'exécution sur ceux-ci des actions. La base de données Journal des événements et statistiques est diffusée sous la forme de réplique et est enregistrée sur chacun des serveurs protégés de l'infrastructure. Elle contient les statistiques cumulées sur tous les événements survenus sur tous les serveurs protégés. Toutes les modifications sont propagées via le mécanisme standard de réplification selon la planification et la topologie.

Les informations sont enregistrées par défaut dans la base de données Journal des événements et statistiques : kaveventslog.nsf.

La base de données Journal des événements et statistiques sert à conserver 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 l'exécution sur ceux-ci des actions. La base de données Journal des événements et statistiques est diffusée sous la forme de répliques et est enregistrée sur chacun des serveurs protégés de l'infrastructure. Elle contient les statistiques cumulées sur tous les événements sur tous les serveurs protégés, toutes les modifications sont diffusées via le mécanisme standard de réplification conformément à la programmation et à la topologie.

Dans le cadre du schéma 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 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 informations conservées dans la base de données Journal des événements et statistiques est possible uniquement via les éléments de l'interface utilisateur de la base de données Centre d'administration. La consultation et la suppression des informations sont réalisées à l'aide des outils de Kaspersky Anti-Virus (cf. rubrique " Consultation de la base de données journal des événements et statistiques " à la page [102](#)).

Le journal des événements reprend les informations qui illustrent l'activité des modules de Kaspersky Anti-Virus au niveau des tâches de serveur Domino (cf. rubrique " Architecture de l'application " à la page [20](#)).

Le détail des informations consignées dans le journal des événements est défini par l'option **Niveau de détail**. Par défaut, les informations les plus importantes sur le fonctionnement de tous les modules de Kaspersky Anti-Virus sont conservées : événements critiques indiquant des problèmes dans le fonctionnement de l'application ou des vulnérabilités dans la protection du serveur.

Le niveau de détail des informations dans le journal, l'emplacement d'affichage des informations sur les événements et la durée de conservation des entrées dans la base de données kaveventslog.nsf sont définis par les paramètres du journal des événements (cf. rubrique " Configuration des paramètres du journal des événements " à la page [96](#)). 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. Les informations reprises dans les statistiques sont définies par le profil dans les paramètres de la protection du courrier, de la protection des réplifications et de l'analyse des bases de données. Par défaut, les informations obtenues suite à l'analyse des objets réparables, irréparables et potentiellement infectés sont conservées, ainsi que les informations sur les objets non analysés avec 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. Une fois ce délai écoulé, les entrées sont supprimées automatiquement. Vous pouvez modifier la durée de conservation des événements et des statistiques aussi bien via le profil que via les paramètres du serveur (cf. rubrique " Configuration

des paramètres du journal des événements " à la page [96](#), " Configuration des paramètres des statistiques " à la page [98](#)).

Pour chaque serveur protégé, il est également possible de supprimer manuellement des informations relatives à ce serveur dans la base de données Journal des événements et statistiques (cf. rubrique " Suppression des informations de la base de données Journal des événements et statistiques " à la page [101](#)).

Les événements enregistrés sur le serveur protégé au cours de la session active de l'application peuvent également apparaître sur la console du serveur Domino et être enregistrés dans un fichier journal au format texte (cf. rubrique " Configuration des paramètres du journal des événements " à la page [96](#)). Par défaut, le système utilise cinq fichiers de journal écrasés de manière cyclique avec le nom server.log_N, où N est le numéro de séquence du log. Les fichiers journaux se trouvent sur le serveur protégé dans le répertoire de service de Kaspersky Anti-Virus (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. rubrique " Administration des paramètres du fichier de configuration notes.ini " à la page [26](#)).

DANS CETTE SECTION

Configuration des paramètres du journal des événements	96
Configuration des paramètres des statistiques.....	98
Suppression des informations de la base de données Journal des événements et statistiques	101
Consultation de la base de données Journal des événements et statistiques.....	102

CONFIGURATION DES PARAMÈTRES DU JOURNAL DES ÉVÉNEMENTS

Kaspersky Anti-Virus permet de 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, sous l'onglet **Paramètres généraux**, décochez la case **Utiliser les paramètres du profil**.

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un profil si vous configurez les paramètres du journal des événements pour un groupe de serveurs, ou un serveur si vous configurez le journal des événements pour un serveur distinct.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-après).

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 (cf. ill. ci-après). Si vous souhaitez utiliser les valeurs des paramètres définis par le profil pour le serveur, cochez la case **Utiliser les paramètres du profil**.

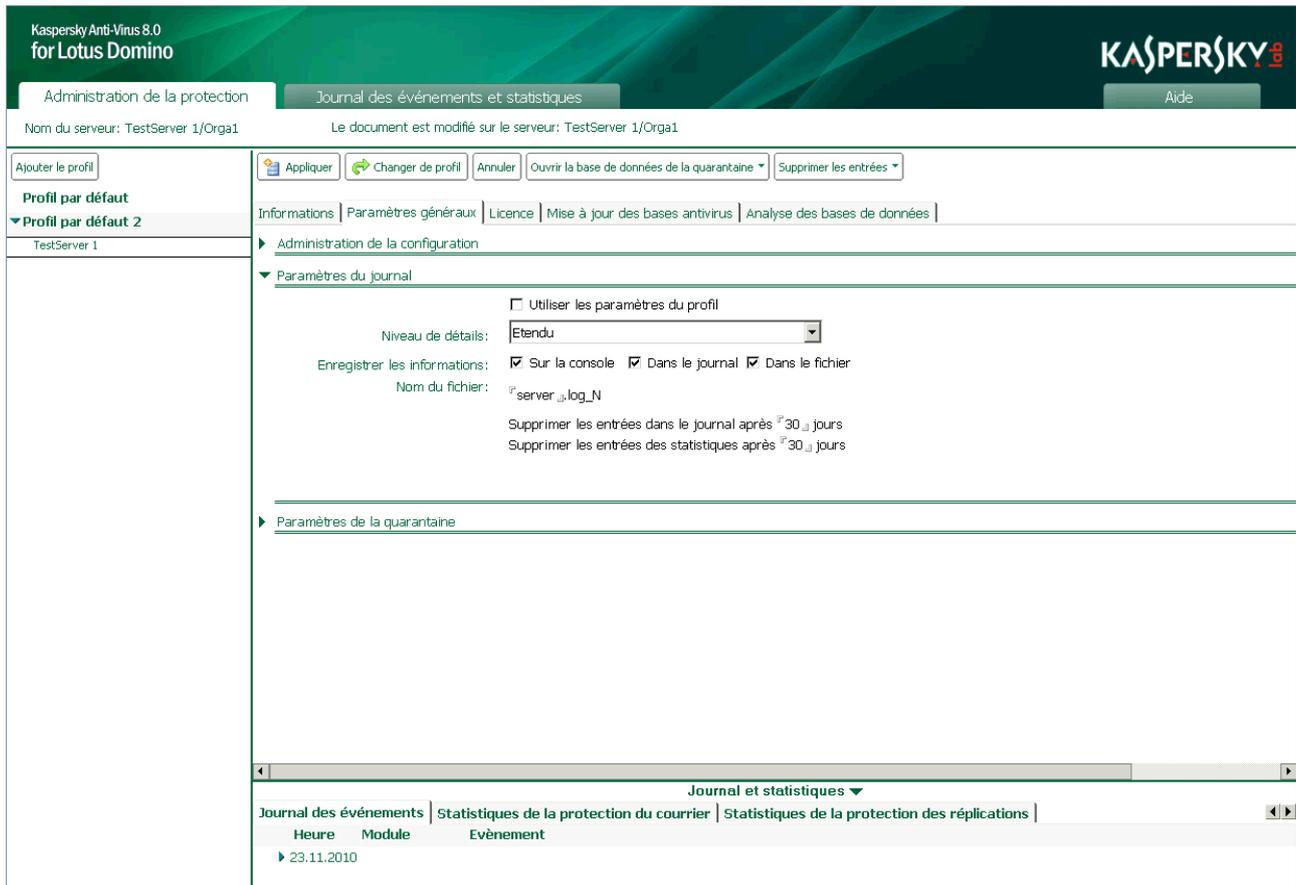


Illustration 36 : Configuration des paramètres du journal des événements pour un serveur en particulier

4. Dans le groupe **Paramètres du journal** (cf. ill. ci-dessus), définissez les valeurs pour les paramètres suivants :
 - Le degré de détail des informations consignées dans le journal. Pour ce faire, sélectionnez une des valeurs suivantes dans la liste **Niveau de détails** :
 - **Standard** : consigner les **événements critiques** ainsi que les événements auxquels il faut absolument prêter attention car ils indiquent des situations importantes dans le fonctionnement de l'application (par exemple, **erreur de connexion à la source de mise à jour**). Cette valeur est choisie par défaut. Dans ini KAVDefaultLogLevel valeur du paramètre : 0.
 - **Etendu** : consigner les événements critiques signalant des vulnérabilités dans la protection du serveur ou des problèmes dans le fonctionnement de l'application ; consigner les informations relatives au fonctionnement de tous les modules de Kaspersky Anti-Virus. Dans ini KAVDefaultLogLevel valeur du paramètre : 1.
 - **Débogage** : consigner les **événements critiques**, les **événements importants** et les événements informatifs, par exemple **L'objet est sain**, **Le module de mise à jour est chargé**. Dans ini KAVDefaultLogLevel valeur du paramètre : 2.

- Emplacement des informations sur les événements enregistrés. Pour ce faire, cochez les cases suivantes dans le groupe **Enregistrer les informations** :
- **Dans le journal** : les informations relatives aux événements seront conservées 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. rubrique " Consultation de la base de données Journal des événements et statistiques " à la page [102](#)).

La base de données kaveventslog.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).

- **Sur la console** : les informations relatives aux événements survenus pendant le fonctionnement de Kaspersky Anti-Virus sont affichées sur la console du serveur Domino. Les informations fournies concernent la séance actuelle d'utilisation de l'application. Le niveau de détail des informations est sélectionné par l'utilisateur.
- **Dans le fichier** : les informations relatives aux événements sont consignées dans un fichier texte du journal. Par défaut, le système utilise cinq fichiers de journal écrasés de manière cyclique avec le nom server.log_N, où N est le numéro de séquence du log. Les fichiers journaux se trouvent sur le serveur protégé dans le répertoire de service de Kaspersky Anti-Virus (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 de la famille Microsoft Windows, dans le répertoire des fichiers binaires du serveur Domino (chemin par défaut : C:\Program Files\Lotus\IBM\Domino\kavcommon) ; pour les systèmes d'exploitation de la famille Linux : dans le répertoire de données du serveur Domino (chemin par défaut : /local/notesdata/kavcommon).

La taille des fichiers journaux est définie dans le fichier de configuration notes.ini (paramètre KAVLogFileSize). La consultation du fichier s'opère via les outils standard 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**. Le fichier indiqué sera créé dans le répertoire logs de Kaspersky Anti-Virus. La modification du nom du fichier via le profil n'est pas possible.

- Durée de conservation des entrées du journal des événements dans la base de données kaveventslog.nsf. Pour ce faire, indiquez dans le champ **Supprimer les entrées dans le journal** après 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. La durée de conservation par défaut des informations est de 30 jours.
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**.

Les paramètres du journal des événements peuvent également être configurés dans le fichier ini (cf. rubrique " Administration des paramètres du fichier de configuration notes.ini " à la page [26](#)).

CONFIGURATION DES PARAMÈTRES DES STATISTIQUES

Kaspersky Anti-Virus permet de tenir des statistiques séparées sur les menaces découvertes et les actions exécutées pour chaque composant de la protection. Par défaut, les informations obtenues suite à l'analyse des objets réparables, irréparables et potentiellement infectés sont conservées, ainsi que les informations sur les objets non analysés avec une explication sur les raisons de l'échec de l'analyse.

Les informations reprises dans les statistiques sont définies par le profil dans les paramètres de la protection du courrier, de la protection des répliquions et de l'analyse des bases de données. La configuration de paramètres individuels de la conservation des statistiques pour le serveur n'est pas prévue.

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 via le profil que pour chaque serveur séparément, dans les paramètres du serveur. 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, sous 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. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez un profil si vous configurez les statistiques pour un groupe de serveurs, ou un serveur si vous configurez les statistiques pour un serveur distinct.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux** (cf. ill. ci-après).

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 (cf. ill. ci-après). Si vous souhaitez utiliser les valeurs des paramètres définis par le profil pour le serveur, cochez la case **Utiliser les paramètres du profil**.

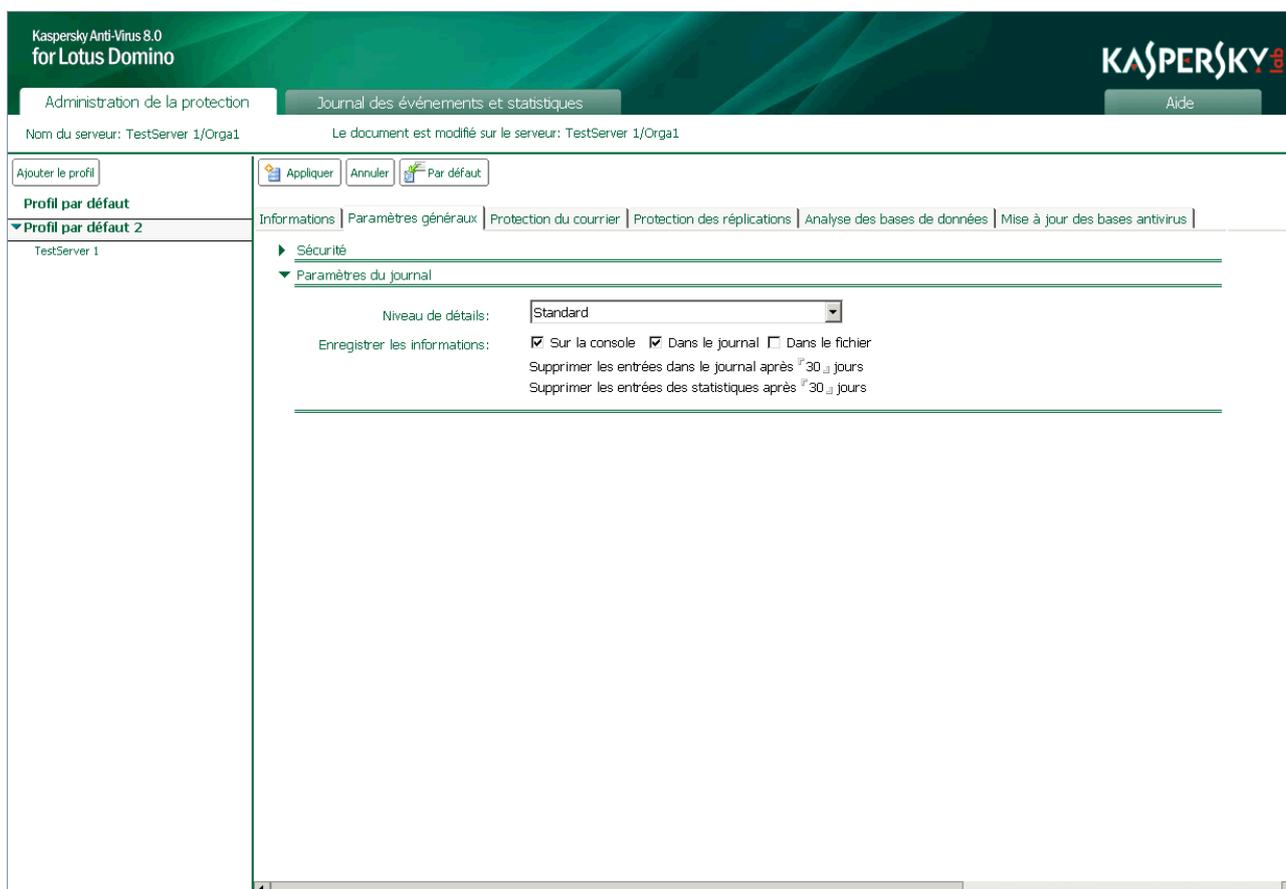


Illustration 37 : Configuration de la durée de conservation des statistiques

4. 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).

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

► Pour définir les données statistiques qui seront conservées dans la base de données Journal des événements et statistiques, 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 modifier les paramètres.
3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier/Protection des réplifications/Analyse des bases de données**, sélectionnez l'onglet **Actions** (cf. ill. ci-après).

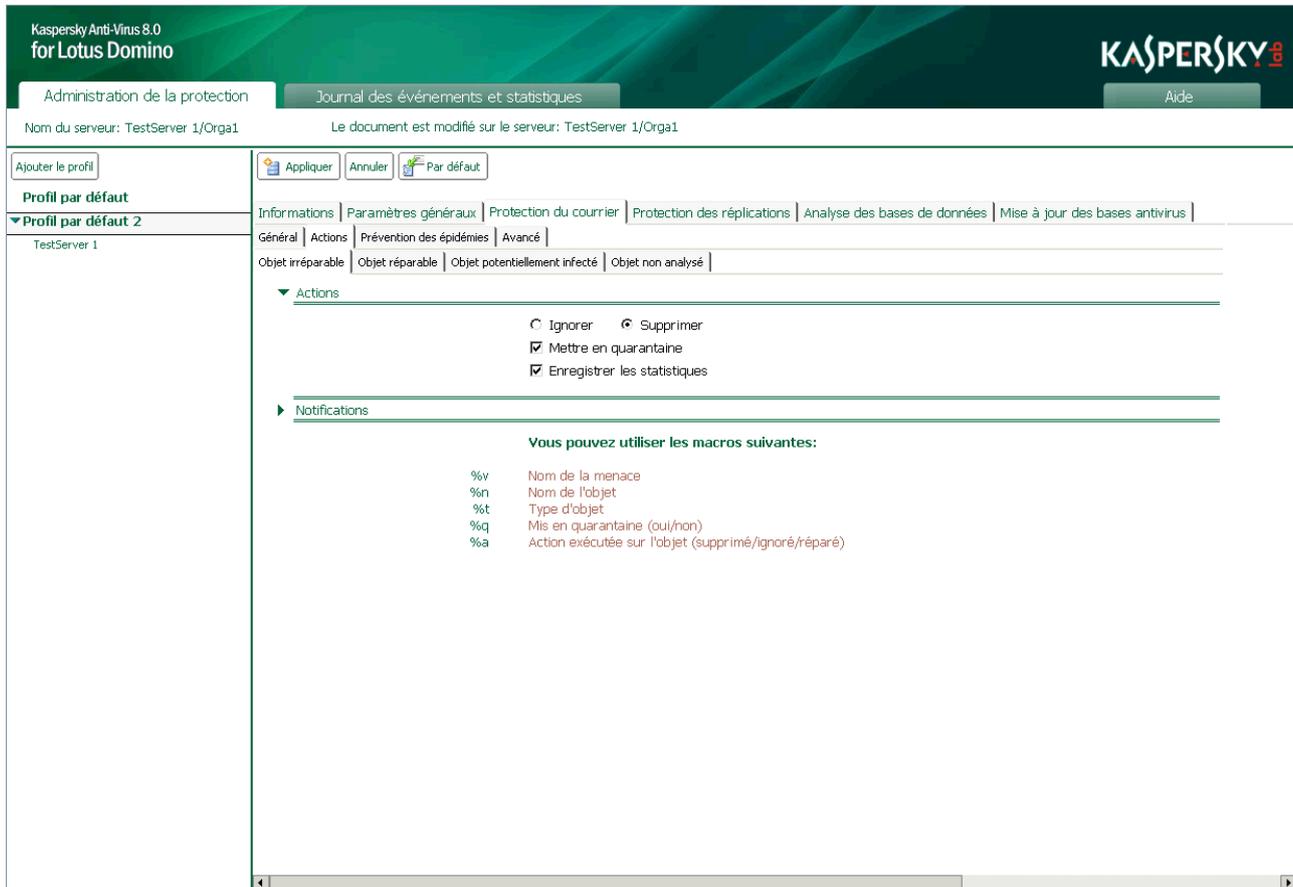


Illustration 38 : Configuration des paramètres de conservation des statistiques

4. Sous l'onglet **Actions**, sélectionnez l'onglet correspondant à l'état des objets dont vous souhaitez conserver les informations dans la base de données Journal des événements et statistiques. Vous avez le choix parmi les onglets suivants :
 - **Objet irréparable.**
 - **Objet réparable.**
 - **Objet potentiellement infecté.**
 - **Objet non analysé.**
5. Sous l'onglet sélectionné, dans le groupe **Actions**, cochez la case **Enregistrer les statistiques** afin que les informations relatives aux objets découverts et aux actions exécutées soient conservées dans la base de données Journal des événements et statistiques. S'il n'est pas nécessaire d'enregistrer les informations, décochez la case.

6. 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**.

SUPPRESSION DES INFORMATIONS DE LA BASE DE DONNÉES JOURNAL DES ÉVÉNEMENTS ET STATISTIQUES

Les entrées de la base de données Journal des événements et statistiques sont supprimées automatiquement à l'issue de la période indiquée dans les paramètres du journal des événements et dans les paramètres des statistiques. Toutefois, vous pouvez le cas échéant supprimer les entrées manuellement. La suppression est réalisée pour chaque serveur séparément.

➔ *Pour supprimer manuellement des entrées dans le journal des événements et des statistiques, procédez comme suit :*

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous souhaitez supprimer des entrées dans la base de données Journal des événements et statistiques (cf. ill. ci-après).

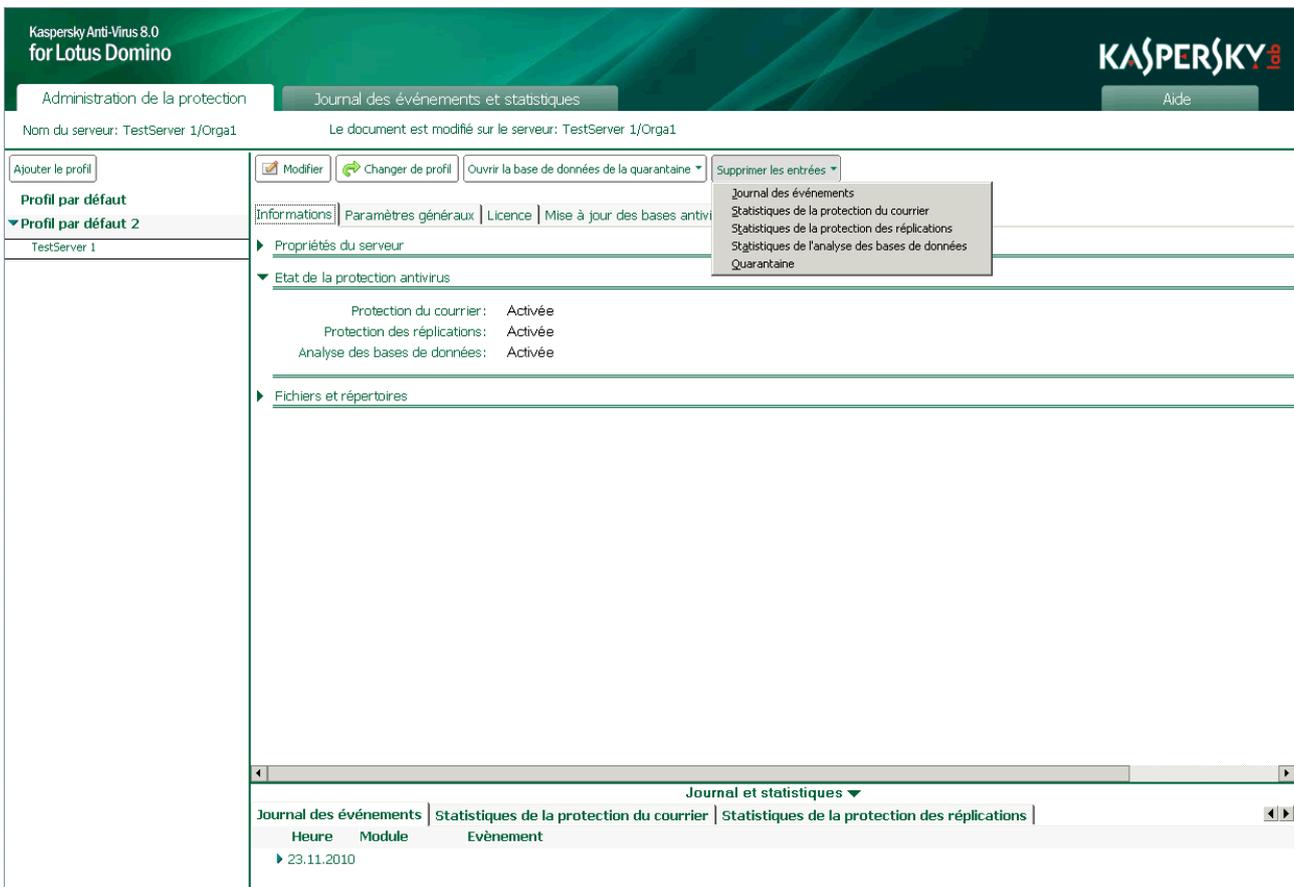


Illustration 39 : Suppression des entrées du journal des événements et statistiques

3. Dans le volet des actions, cliquez sur le bouton **Supprimer les entrées** et dans la liste déroulante, choisissez la valeur souhaitée. La liste contient les éléments pour la suppression des informations suivantes :
 - **Journal des événements.**
 - **Statistiques de la protection du courrier.**

- **Statistiques de la protection des réplifications.**
- **Statistiques de l'analyse des bases de données.**

Les informations correspondantes au point que vous aurez sélectionné seront supprimées de la base de données kaveventslog.nsf sur le serveur sélectionné.

CONSULTATION DE LA BASE DE DONNÉES JOURNAL DES ÉVÉNEMENTS ET STATISTIQUES

Kaspersky Anti-Virus permet de consulter les informations suivantes consignées dans la base de données Journal des applications et statistiques (kaveventslog.nsf) :

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

Sachez que vous pouvez consulter les informations pour un seul serveur (cf. rubrique " Consultation du journal des événements et des statistiques " à la page [105](#)) ou les informations globales sur tous les serveurs (cf. rubrique " Consultation du journal global des événements et des statistiques " à la page [102](#)), quel que soit le profil auquel ils appartiennent.

DANS CETTE SECTION

Consultation du journal global des événements et des statistiques	102
Consultation du journal des événements et des statistiques pour le serveur	105

CONSULTATION DU JOURNAL GLOBAL DES ÉVÉNEMENTS ET DES STATISTIQUES

➤ *Pour consulter le journal global des événement 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 rubrique contenant les informations qui vous intéressent : **Journal des événements, Statistiques de la protection du courrier, Statistiques de l'analyse des bases de données, Statistiques de la protection des réplifications.**
3. Choisissez une des sections reprises dans la rubrique.

Les entrées de la section sélectionnée apparaîtront dans la zone de consultation. 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 regroupée, cliquez sur l'icône . Pour réduire la liste des événements, cliquez sur l'icône .

Les entrées du tableau 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.

JOURNAL DES ÉVÉNEMENTS

La rubrique **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 (**Evènements critiques**, **Evènements importants**, **Evènements informatifs**).

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

Les informations suivantes sont reprises pour chaque événement dans les sections du journal :

- Icône illustrant le degré d'importance de l'événement :
 -  – *événement critique*. Événement 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*. Événement 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*. Événement 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.
- **Événement** : description de l'événement enregistré, reprend le type d'événement et des informations complémentaires à son sujet.

Les entrées du tableau 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 rubriques des statistiques contiennent les sections suivantes :

- **Général** : statistiques complètes de la rubrique 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 des objets.
- **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 nom des bases de données dans lesquelles des documents infectés ont été découverts (uniquement pour les statistiques de la protection des répliquions 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 répliquions 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 reprises pour chaque événement dans les rubriques des statistiques :

- Icône indiquant l'état de l'objet analysé :
 -  – objet réparé ;
 -  – objet non 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 répliquions et de l'analyse des bases de données).
- **Module** : nom du module ayant analysé l'objet.
- **Menace** : nom de la menace, si l'objet analysé était infecté. Si l'objet n'était pas infecté, son nom et l'état attribué à l'issue de l'analyse antivirus seront affichés.
- **Auteur des modifications** : nom de l'utilisateur qui a introduit les dernières modifications dans le document et nom du serveur sur lequel elles ont été réalisées. Format de l'entrée : **<NomUtilisateur/NomServeur>** (uniquement pour les statistiques de la protection des répliquions et l'analyse des bases de données).

Les entrées du tableau 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 ÉVÉNEMENTS ET DES STATISTIQUES POUR LE SERVEUR

► *Pour consulter le journal des événements et les statistiques pour chaque serveur, procédez comme suit :*

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

Les entrées de la base de données du journal des événements et des statistiques sont affichées dans la zone de consultation sous les onglets : **Journal des événements**, **Statistiques de la protection du courrier**, **Statistiques de la protection des répliquions** et **Statistiques de l'analyse des bases de données**.

L'onglet sélectionné affichera les mêmes informations que dans le journal des événements (cf. rubrique " Journal des événements " à la page [103](#)) global et que dans les statistiques générales (cf. rubrique " Statistiques " à la page. [103](#)), mais uniquement pour le serveur que vous aurez sélectionné.

Les entrées sur tous les onglets sont regroupées par date d'enregistrement. Les statistiques de la protection du courrier sont également regroupées selon les adresses électroniques des expéditeurs des messages, et les statistiques de la protection des répliquions et d'analyse des bases de données sont regroupées selon le nom des bases de données dans lesquelles se trouvent les documents. Pour ouvrir la liste complète, cliquez sur l'icône ▶. Pour réduire la liste, cliquez sur l'icône ▼.

NOTIFICATIONS

Kaspersky Anti-Virus peut signaler la découverte des objets suivants lors de l'analyse des messages électroniques, des répliquions et des bases de données :

- **Objet irréparable.**
- **Objet réparable.**
- **Objet potentiellement infecté.**
- **Objet non analysé.**

Si l'analyse des messages électroniques a mis en évidence une augmentation du nombre d'objets infectés ou endommagés ou d'objets contenant la même menace, Kaspersky Anti-Virus peut prévenir les administrateurs de l'épidémie (cf. rubrique " Notifications sur les épidémies " à la page [66](#)). Les critères de notification d'une épidémie sont définis par l'administrateur pour chaque catégorie d'objet séparément.

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

Dans le cadre de l'analyse des messages électroniques, les informations peuvent être ajoutées au corps du message analysé. L'expéditeur et les destinataires de ce message, ainsi que les administrateurs du serveur et les administrateurs du profil auquel appartient ce serveur, peuvent recevoir une notification rédigée selon un modèle défini dans les paramètres de la protection du courrier.

Dans le cadre de l'analyse des répliquions 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 répliquions et dans les paramètres d'analyse des bases de données.

Les administrateurs de serveur sont désignés dans les paramètres du serveur (cf. rubrique " Désignation de l'administrateur de serveur " à la page [111](#)) : sous l'onglet **Informations** dans le groupe **Propriétés du serveur**. Les administrateurs de profil sont désignés dans les paramètres du profil (cf. rubrique " Désignation de l'administrateur de profil " à la page [111](#)) : sous l'onglet **Paramètres généraux** dans le groupe **Sécurité**.

Les paramètres de notification sur les objets irréparables, réparables, potentiellement infectés et non analysés découverts sont définis pour chaque état séparément dans les paramètres de la protection du courrier, de la protection des répliquions 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 la notification pour le serveur n'est pas prévue.

➡ *Pour configurer les paramètres de notification, 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 modifier les paramètres.

3. Dans le volet des actions, cliquez sur **Modifier** et dans la zone d'administration, sous l'onglet **Protection du courrier/Protection des répliquions/Analyse des bases de données**, sélectionnez l'onglet **Actions** (cf. ill. ci-après).

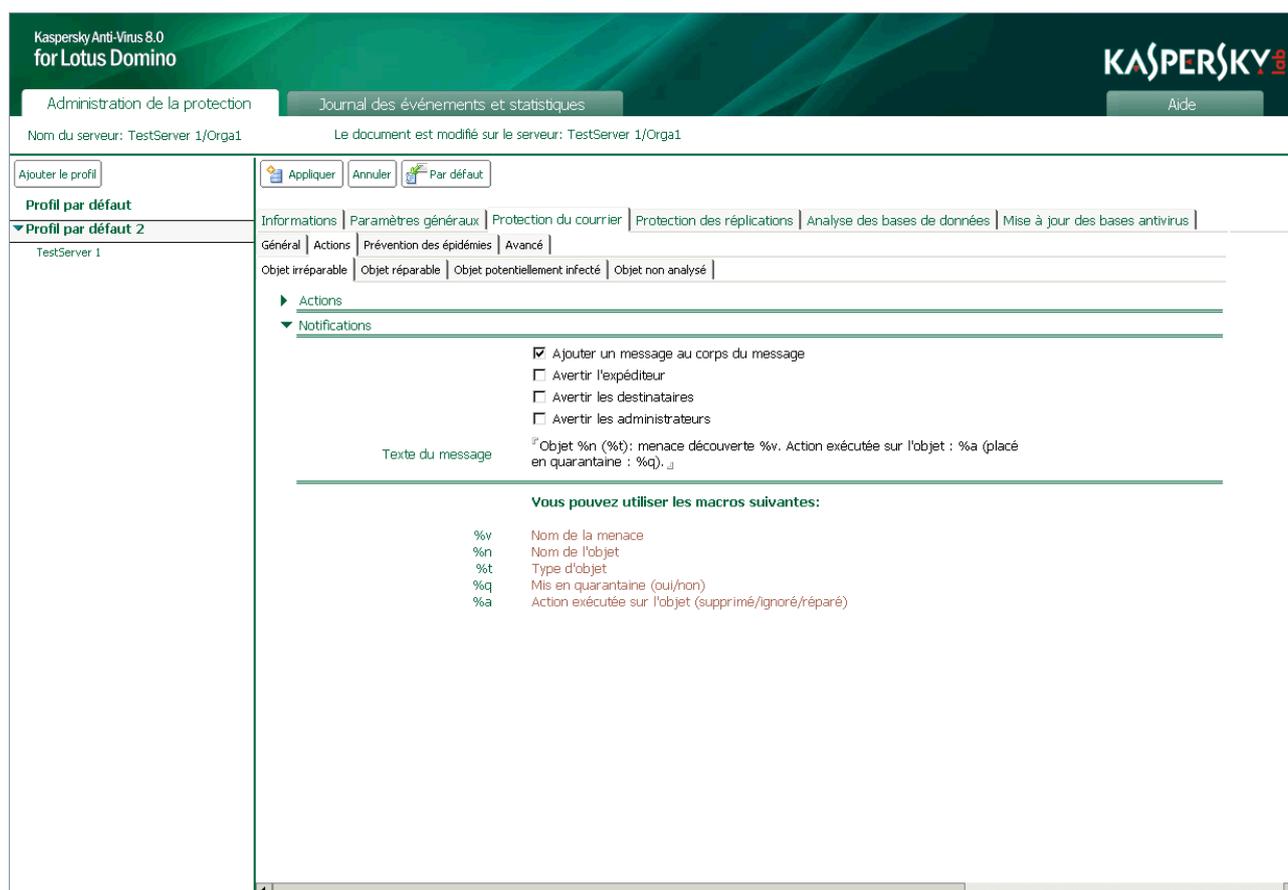


Illustration 40 : Configuration des notifications

4. Sous l'onglet **Actions**, sélectionnez l'onglet correspondant à l'état des objets pour lesquels vous souhaitez configurer les notifications. Vous avez le choix parmi les onglets suivants :
 - **Objet irréparable** : configuration des paramètres de notification sur les objets infectés irréparables.
 - **Objet réparable** : configuration des paramètres de notification sur les objets infectés réparables.
 - **Objet potentiellement infecté** : configuration des paramètres de notification sur les objets potentiellement infectés.
 - **Objet non analysé** : configuration des paramètres de notification sur les objets non analysés.
5. Dans le groupe **Notification** (cf. ill. ci-dessus), configurez les paramètres selon lesquels les notifications sur les objets découverts et les actions exécutées seront réalisées. Pour ce faire, cochez ou décochez les cases suivantes :
 - **Ajouter un message au corps du message** : ajouter au corps de texte du message original un message saisi dans le champ **Texte du message** du modèle.
 - **Avertir l'expéditeur** : envoyer à l'expéditeur un message électronique contenant le texte défini dans le champ **Texte du message** du modèle.
 - **Avertir les destinataires** : envoyer aux destinataires un message électronique contenant le texte défini dans le champ **Texte du message** du modèle.

- **Avertir les administrateurs** : envoyer un message électronique aux administrateurs du serveur et aux administrateurs du profil auquel le serveur appartient rédigé selon le champ **Texte du message** du modèle.

Les administrateurs de serveur sont désignés dans les paramètres du serveur (cf. rubrique " Désignation de l'administrateur de serveur " à la page [111](#)) : sous l'onglet **Informations** dans le groupe **Propriétés du serveur**. Les administrateurs de profil sont désignés dans les paramètres du profil (cf. rubrique " Désignation de l'administrateur de profil " à la page [111](#)) : sous l'onglet **Paramètres généraux** dans le groupe **Sécurité**.

Dans le champ **Texte du message**, rédigez le texte qui sera ajouté en guise de notification. Vous pouvez utiliser les champs suivants :

- **%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 ;
 - **%d** : informations sur la suppression de l'objet : **oui** , l'objet est supprimé, **non** , l'objet n'a pas été supprimé.
6. 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

Les paramètres de fonctionnement de Kaspersky Anti-Virus sont définis via les paramètres des profils et les paramètres des serveurs (cf. rubrique " Administration des paramètres de Kaspersky Anti-Virus " à la page [24](#)).

Le profil permet de définir des paramètres uniques 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 requises (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

Création et suppression de profils	109
Désignation de l'administrateur de profil	111
Désignation de l'administrateur de serveur.....	111
Déplacement du serveur vers un autre profil.....	112
Définition de valeurs individuelles pour les paramètres du serveur	112
Exploitation de la possibilité de modification directe des paramètres du serveur	114

CRÉATION ET SUPPRESSION DE PROFILS

L'autorisation de créer ou de supprimer un profil est accordée uniquement aux utilisateurs qui possèdent les privilèges des groupes fonctionnels **Administrateurs de la sécurité** et **Administrateurs du Centre d'administration**.

➔ *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 seront affichés dans la zone d'administration. Le profil est créé par défaut avec les valeurs recommandées par les experts de Kaspersky Lab. Vous pouvez modifier les paramètres du profil.

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

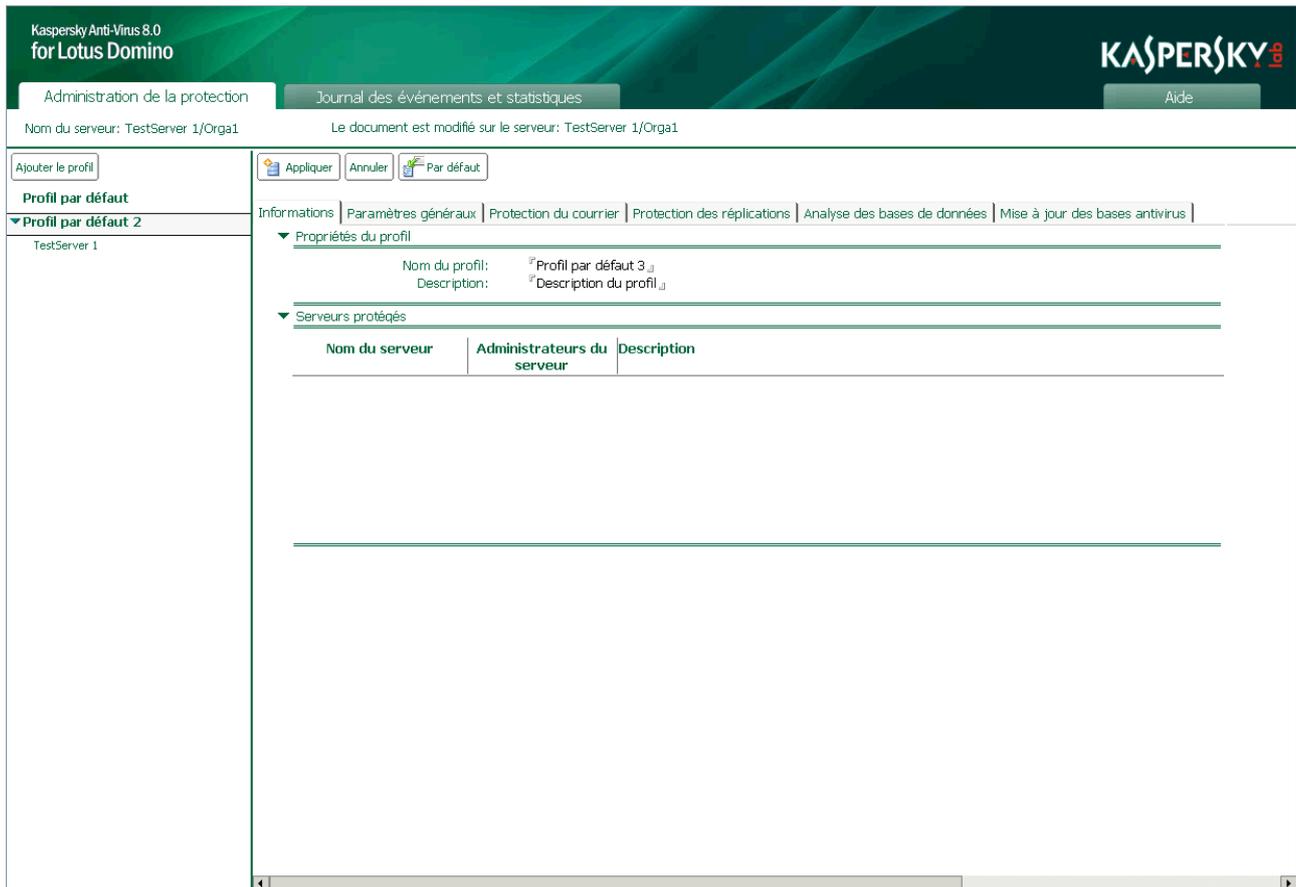


Illustration 41 : Configuration du profil

4. 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 seront ajoutées à la réplique de la base de données Centre d'administration qui se trouve sur le même serveur où la base de données a été ouverte. Lors de la réplification suivante, les modifications des paramètres seront transmises aux autres serveurs protégés.

➔ *Pour supprimer 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 que vous souhaitez supprimer.

Avant de pouvoir supprimer le profil, tous les serveurs qu'il contient doivent avoir été déplacés vers un autre profil.

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

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

Il est possible également de supprimer un profil à l'aide de l'option **Supprimer** du menu contextuel du profil ou à l'aide de la touche **Delete**. 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**.

DÉSIGNATION DE L'ADMINISTRATEUR DE PROFIL

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, choisissez le profil pour lequel vous souhaitez désigner un administrateur.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux**.
4. Dans le groupe **Sécurité**, indiquez le nom de l'administrateur de profil ou le nom du groupe d'administrateurs d'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 Notes, hiérarchie de l'organisation).
 - Choisissez le nom de l'administrateur ou du groupe d'administrateurs dans le Carnet d'adresses du serveur Domino. Pour ce faire, cliquez sur .

L'administrateur de profil doit être un utilisateur qui possède les privilèges d'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité**, **Administrateurs du Centre d'administration** ou **Administrateurs avec des privilèges restreints**.

Par défaut, les administrateurs sont les utilisateurs ajoutés au groupe **Administrateurs du Centre d'administration** lors de l'installation de l'application.

5. 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**.

DÉSIGNATION DE L'ADMINISTRATEUR DE SERVEUR

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur pour lequel vous voulez désigner un administrateur.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Informations**.
4. Dans le groupe **Sécurité**, indiquez le nom de l'administrateur de serveur ou le nom du groupe d'administrateurs d'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 Notes, hiérarchie de l'organisation).
 - Choisissez le nom de l'administrateur ou du groupe d'administrateurs dans le Carnet d'adresses du serveur Domino. Pour ce faire, cliquez sur .

L'administrateur de serveur doit être un utilisateur qui possède les privilèges d'un des trois groupes fonctionnels suivants : **Administrateurs de la sécurité**, **Administrateurs du Centre d'administration** ou **Administrateurs avec des privilèges restreints**.

Par défaut, les administrateurs de serveur sont les utilisateurs ajoutés au groupe **Administrateurs du Centre d'administration** lors de l'installation de l'application.

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

DÉPLACEMENT DU SERVEUR VERS UN AUTRE PROFIL

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

1. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez dans le profil le serveur que vous voulez déplacer.
3. Dans le volet des actions, cliquez sur le bouton **Changer de profil**.
4. Dans la fenêtre **Changer de profil** qui s'ouvre, sélectionnez dans la liste le profil dans lequel vous souhaitez déplacer le serveur, puis cliquez sur **OK**.

Le serveur sélectionné sera déplacé dans l'autre profil. Lors de la réplication suivante, ces 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 le déplacement du serveur. Si la case **Utiliser les paramètres du profil** n'est pas cochée, les valeurs actuelles des paramètres seront conservées.

DÉFINITION DE VALEURS INDIVIDUELLES POUR LES PARAMÈTRES 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 de la mise à jour des bases antivirus ;
 - paramètres de la connexion à la source de la mise à jour ;
 - programmation de la mise à jour ;
- Paramètres du journal des événements et des statistiques :
 - degré de détail des informations consignées 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. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez le profil auquel appartient le serveur dont vous souhaitez modifier les paramètres individuels.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et dans la zone d'administration, sélectionnez l'onglet **Mise à jour des bases antivirus**.
4. Dans le groupe **Paramètres de la mise à jour**, décochez la case **Utiliser les paramètres du profil** (cf. ill. ci-après).

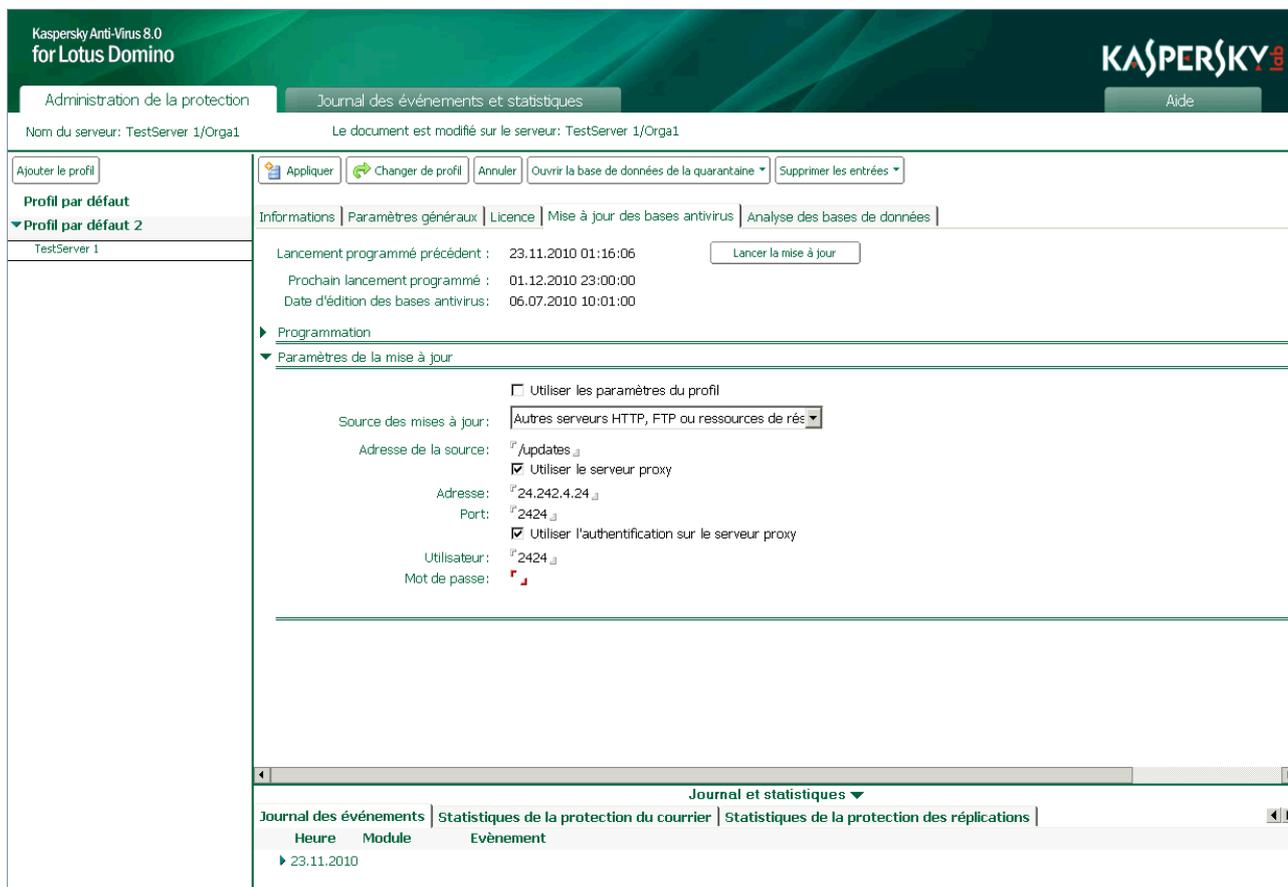


Illustration 42 : Configuration des paramètres individuels de mise à jour pour le serveur

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

5. Pour chaque serveur, désignez les paramètres de la mise à jour des bases antivirus (cf. rubrique " Sélection de la source des mises à jour " à la page 53) ou programmez la mise à jour (cf. rubrique " Mise à jour selon la programmation " à la page 54).
 6. 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. Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.
2. Dans le volet de navigation, sélectionnez le profil auquel appartient le serveur dont vous souhaitez modifier les paramètres individuels.

- Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux**.
- Dans le groupe **Paramètres du journal**, décochez la case **Utiliser les paramètres du profil** (cf. ill. ci-après).

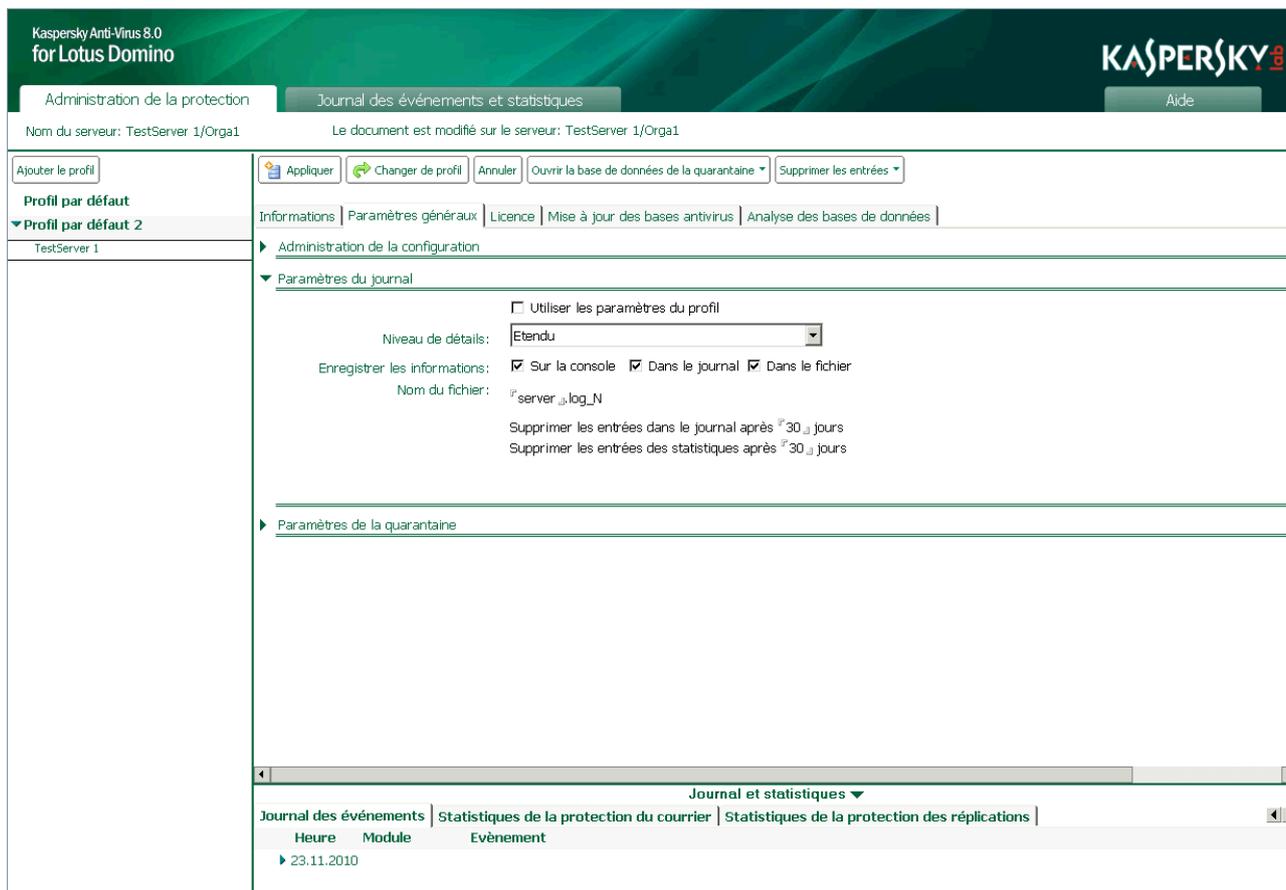


Illustration 43 : Configuration des valeurs individuelles des paramètres du journal des événements et statistiques pour le serveur

- Configurez les paramètres du journal des événements (cf. rubrique " Configuration des paramètres du journal des événements " à la page [96](#)) ou les paramètres de conservation des statistiques (cf. rubrique " Configuration des paramètres des statistiques " à la page [98](#)).
- Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

EXPLOITATION DE LA POSSIBILITÉ DE MODIFICATION DIRECTE DES PARAMÈTRES DU SERVEUR

Par défaut, les modifications des paramètres du serveur sont introduites dans la réplique de la base de données située sur le même serveur que celui auquel la connexion a été réalisée. Si vous configurez les paramètres du serveur via le client Lotus Notes, les modifications 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 sur le serveur protégé seront appliquées bien plus vite. En cas d'utilisation via le navigateur Internet, les modifications des paramètres du serveur sont toujours introduites dans la réplique de la base de données, située sur ce serveur auquel la connexion a été réalisée.

➔ *Pour modifier les paramètres du serveur dans la réplique de la base de données Centre d'administration sur le serveur dont vous modifiez les paramètres, procédez comme suit :*

- Dans le volet de transfert, choisissez l'onglet **Administration de la protection**.

2. Dans le volet de navigation, sélectionnez dans le profil le serveur dont vous souhaitez configurer les paramètres.
3. Dans le volet des actions, cliquez sur le bouton **Modifier** et choisissez, dans la zone d'administration, l'onglet **Paramètres généraux**.
4. Dans le groupe **Administration de la configuration**, décochez la case **Modifier le document sur le serveur protégé**.
5. Dans le volet des actions, cliquez sur **Appliquer** pour enregistrer les modifications introduites.

VALIDATION DE LA CONFIGURATION DE L'APPLICATION

DANS CETTE SECTION

Virus d'essai EICAR et ses modifications	116
Test de la protection du courrier	117
Test de la protection des répliques	118
Test de l'analyse des bases de données.....	118

VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

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

Le virus d'essai 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 d'authentiques virus pour vérifier le fonctionnement de votre antivirus !

Vous pouvez télécharger le " virus " 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 faut absolument 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 virus 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 virus d'essai standard afin de vérifier le bon fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut modifier le contenu du virus standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le **Bloc-Notes de Microsoft** ou **VIM UltraEdit32**, etc.

Vous pouvez vérifier le bon fonctionnement de votre logiciel antivirus à l'aide d'une modification du virus 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 contient les préfixes qu'il faut ajouter en tête de la ligne du virus 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 virus d'essai, enregistrez le fichier, par exemple sous le nom : *ecar_dele.com*. Nommez tous les virus modifiés selon le même principe.

Tableau 6. Modifications du virus d'essai

PRÉFIXE	ÉTAT DE L'OBJET	INFORMATIONS RELATIVES AU TRAITEMENT DE L'OBJET
Pas de préfixe, "virus" d'essai standard.	Irréparable. L'objet contient le code d'un virus connu. Réparation impossible.	Kaspersky Anti-Virus identifie l'objet comme un virus qui ne peut être réparé et applique l'action pour les objets irréparables.
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-	Suspect. L'objet contient le code d'un virus inconnu. Réparation impossible.	L'analyseur heuristique attribue l'état suspect 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.
	Suspect. 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.
ERRO-	Erreur d'analyse. 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 multivolume) ou il n'y a pas de lien vers l'objet.
CURE-	Réparable. L'objet contient le code d'un virus connu. Réparable.	L'objet contient un virus qui peut être réparé. Kaspersky Anti-Virus répare l'objet et le texte du corps du " virus " est remplacé par CURE.

TEST DE LA PROTECTION DU COURRIER

Pour tester l'identification de virus dans les messages électroniques, vous pouvez utiliser n'importe quel système de messagerie qui utilise un serveur Domino protégé. Il est conseillé de vérifier le fonctionnement de Kaspersky Anti-Virus aussi bien dans le corps du message que dans les pièces jointes. Pour vérifier la découverte de virus dans le corps des messages, placer le texte du virus d'essai standard ou d'une de ses modifications dans le corps du message.

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

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

Kaspersky Anti-Virus découvre un objet, l'identifie comme irréparable et en cas d'utilisation d'un virus modifié à l'aide d'un préfixe (cf. rubrique " Virus d'essai EICAR et ses modifications " à la page [116](#)) puis exécute l'action sélectionnée dans les paramètres de la protection du courrier pour ce genre d'objet. Par défaut, l'objet irréparable est supprimé du message électronique.

TEST DE LA PROTECTION DES RÉPLICATIONS

Il est conseillé de vérifier l'identification des virus dans le texte au format Rich Text, dans les pièces jointes et dans les objets OLE.

► *Pour vérifier la découverte de virus lors de la réplication, procédez comme suit :*

1. Sélectionnez le serveur avec lequel la réplication est configurée sur le serveur protégé.
2. Sélectionnez, sur le serveur, la base de données dont la réplique se trouve sur le serveur protégé, puis choisissez le document contenant le champ RTF. Ou créez sur le serveur non protégé une base de données sur la base d'un des modèles proposés, puis sur le serveur protégé, créez la réplique de cette base, puis créez dans la base du serveur non protégé un document contenant le champ RTF.
3. Placez le texte du virus d'essai standard ou modifié dans le champ RTF du document sélectionné.
4. Ajoutez au document sélectionné un fichier et un objet OLE contenant le texte du virus d'essai standard ou modifié.

À la prochaine réplication, Kaspersky Anti-Virus découvrira les objets, les identifiera comme irréparables et, en cas d'utilisation du virus modifié à l'aide des préfixes (cf. rubrique " Virus d'essai EICAR et ses modifications " à la page [116](#)), puis exécutera les actions sélectionnées dans les paramètres de la protection des réplications pour ces objets. Par défaut, les objets irréparables sont supprimés, les informations relatives à la découverte 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.

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

TEST DE L'ANALYSE DES BASES DE DONNÉES

Il est conseillé de vérifier l'identification des virus dans le texte au format Rich Text, dans les pièces jointes et dans les objets OLE.

► *Pour vérifier la découverte de virus pendant l'analyse des bases de données, procédez comme suit :*

1. Sélectionnez une base de données sur le serveur, puis choisissez un document contenant un champ RTF ou créez une base de données sur la base d'un des modèles existants et créez-y un document contenant un champ RTF.
2. Placez le texte du virus d'essai standard ou modifié dans le champ RTF du document sélectionné.
3. Ajoutez au document sélectionné un fichier et un objet OLE contenant le texte du virus d'essai standard ou modifié.

À la prochaine réplication, Kaspersky Anti-Virus découvrira les objets, les identifiera comme irréparables et, en cas d'utilisation du virus modifié à l'aide des préfixes (cf. rubrique " Virus d'essai EICAR et ses modifications " à la page [116](#)), puis exécutera les actions sélectionnées dans les paramètres de la protection des réplications pour ces objets. Par défaut, les objets irréparables sont supprimés, les informations relatives à la découverte 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.

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 principales de Kaspersky Anti-Virus via la ligne de commande de la console de serveur Domino. Cette rubrique reprend les instructions système qui permettent d'administrer les fonctions de Kaspersky Anti-Virus.

Les instructions système sont saisies uniquement pour la tâche kavcontrol sur chaque serveur séparément.

L'instruction doit respecter la syntaxe suivante :

```
tell kavcontrol <instructions> [<paramètre>]
```

où

- `instruction` est l'instruction de Kaspersky Anti-Virus ;
- `paramètre` désigne le paramètres indispensable à l'exécution de l'instruction (le cas échéant).

S'il faut 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. Il faut un espace entre le paramètre et l'instruction.

Exemple :

Correct :

```
tell kavcontrol addlicensekey "/home/petia/my key"
```

Incorrect :

```
tell kavcontrol addlicensekey " /home/petia/my key"
```

Le tableau ci-après reprend la liste des instructions de Kaspersky Anti-Virus.

Tableau 7. Instructions de Kaspersky Anti-Virus

INSTRUCTION	PARAMÈTRES	ACTION
Help		Afficher les commandes disponibles.
AddLicenseKey	<chemin_complet_au_fichier_de_licence_sur_le_serveur>	Ajouter un fichier de licence.
DelFirstKey		Supprimer le fichier de licence actif.
DelSecondKey		Supprimer le fichier de licence de réserve.
ShowLicense		Afficher les informations sur la clé active.
StartScanner		Lancer l'analyse des bases de données.
StopScanner		Arrêter l'analyse des bases de données.
PauseScanner		Suspendre l'analyse des bases de données.
ResumeScanner		Reprendre l'analyse des bases de données.
StartUpdater		Lancer la mise à jour des bases antivirus.
StopUpdater		Arrêter la mise à jour des bases antivirus.
ShowVersion		Afficher le numéro de la version de Kaspersky Anti-Virus installée sur le serveur.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

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

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et en cas d'infection, ils vous aideront à supprimer les dégâts provoqués par les applications malveillantes.

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

Requête électronique adressée au Service d'assistance technique

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

Pour envoyer une requête par voie électronique, vous devez indiquer le **numéro de client** obtenu lors de l'enregistrement sur le site Internet du service d'assistance technique ainsi que le **mot de passe**.

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

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

Décrivez le plus exactement possible le problème que vous rencontrez. Dans les champs obligatoires, indiquez :

- **Le type de requête.** Sélectionnez le sujet, qui correspond le mieux au problème rencontré, par exemple, "Problème d'installation/de suppression du logiciel", ou "Problème de recherche/de neutralisation de virus". Si vous ne trouvez pas un sujet qui se rapproche le plus de votre situation, choisissez "Question générale".
- **Nom et version de l'application.**
- **Texte de la demande.** Décrivez le problème rencontré avec le plus de détails possibles.
- **Numéro de client et mot de passe.** Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement sur le site du service d'assistance technique.
- **Adresse de messagerie.** Il s'agit de l'adresse à laquelle les experts du service d'assistance technique enverront la réponse à votre question.

Assistance technique par téléphone

Si le problème est urgent, vous pouvez contacter le service d'assistance technique dans votre ville. Si vous contactez l'assistance technique (<http://support.kaspersky.com/fr/support/international>) veuillez fournir les informations (<http://support.kaspersky.com/fr/support/details>) relatives à l'ordinateur et au logiciel antivirus installé. Nos experts pourront ainsi vous venir en aide plus rapidement.

GLOSSAIRE

A

ARCHIVE

Fichier contenant un ou plusieurs autres objets qui peuvent à leur tour être des archives.

F

FICHIER DE LICENCE

Fichier portant l'extension *.key et qui est votre " clé " personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. La clé de licence est reprise dans le pack logiciel lorsque vous achetez celui-ci chez un revendeur Kaspersky Lab. Par contre, elle vous sera envoyée par courrier électronique si vous achetez le logiciel en ligne.

I

INTERCEPTEUR

Sous-composant de l'application qui répond à l'analyse de certains types de messages électroniques. L'ensemble des intercepteurs à installer dépend du rôle ou de la combinaison des rôles du déploiement de l'application.

M

MISE À JOUR DES BASES

Une des fonctions des applications de Kaspersky Lab qui permet de maintenir l'actualité de la protection. Les bases sont copiées depuis les serveurs de mises à jour de Kaspersky Lab sur l'ordinateur et elles sont connectées automatiquement à l'application.

O

OBJET OLE

Objet joint ou intégré à un autre fichier. L'application de Kaspersky Lab peut rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Microsoft Office Excel dans un document Microsoft Office Word, ce tableau sera traité comme un objet OLE.

OBJET INFECTÉ

Objet avec le code malveillant : lors de l'analyse d'un objet, une équivalence complète entre un extrait du code de l'objet et un extrait du code d'une menace connue a été découverte. Les experts de Kaspersky Lab vous recommandent de ne pas travailler avec ces objets, car cela peut amener à l'infection de votre ordinateur.

OBJET POTENTIELLEMENT INFECTÉ.

Objet dont le code contient soit le code modifié d'un virus connu, soit le code qui évoque un virus, mais qui n'a pas encore été identifié par Kaspersky Lab. Il est possible que les fichiers infectés soient détectés à l'aide de l'analyse heuristique.

P

PAQUET DE MISES À JOUR

Paquet de fichiers pour la mise à jour de l'application, copié depuis Internet et installé sur l'ordinateur.

Q**QUARANTAINE**

Dossier spécial contenant tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

KASPERSKY LAB

Fondée en 1997, Kaspersky Lab est devenue un leader reconnu en technologies de sécurité de l'information. Elle produit un large éventail de logiciels de sécurité des données et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, contre le courrier indésirable et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve en Fédération de Russie et la société possède des bureaux régionaux au Royaume Uni, en France, en Allemagne, au Japon, aux Etats-Unis (Californie), dans les pays du Benelux, en Chine, en Pologne et en Roumanie. Un nouveau service de la compagnie, le centre européen de recherches antivirus, a été récemment ouvert en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises à travers le monde.

Aujourd'hui, Kaspersky Lab emploie plus de 1 000 spécialistes hautement qualifiés : 10 d'entre eux possèdent un M.B.A et 16 autres, un doctorat. Les principaux experts de Kaspersky Lab sont membres de la prestigieuse Computer Anti-virus Researcher's Organization (organisation pour la recherche antivirus en informatique, CARO).

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

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de protection contre les virus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les normes de protection contre les virus en vigueur aujourd'hui. Le produit vitrine de la société est Kaspersky Antivirus : il assure la protection de tous les objets qui peuvent être pris pour cible par les virus, à savoir les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui sont parfaitement ajustés aux besoins spécifiques des activités professionnelles. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection contre les virus pour entreprise. Les bases antivirus de Kaspersky Lab sont mises à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

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

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

Encyclopédie des virus : <http://www.securelist.com>

Laboratoire d'étude des virus : newvirus@kaspersky.com
(envoi uniquement d'objets suspects sous forme d'archive)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>
(pour les questions aux experts antivirus)

INFORMATIONS SUR LE CODE TIERS

Du code développé par des éditeurs tiers a été utilisé dans cette application.

DANS CETTE SECTION

Code logiciel.....	125
Outils de développement.....	138
Informations diverses	142

CODE LOGICIEL

Informations relatives au code utilisé dans cette application et développés par des éditeurs tiers.

BOOST 1.30

Copyright (C) 2003, Christof Meerwald

EXPAT 1.2

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GECKO SDK 1.8

Copyright (C) 1998-2008, Mozilla Foundation

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use"

means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor"

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

1.2. "Contributor Version"

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

1.3. "Covered Code"

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

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

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

1.7. "Larger Work"

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

1.8. "License"

means this document.

1.8.1. "Licensable"

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

1.9. "Modifications"

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

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

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

1.10. "Original Code"

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

1.10.1. "Patent Claims"

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

1.11. "Source Code"

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

1.12. "You" (or "Your")

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

2. Source Code License.

2.1. The Initial Developer Grant.

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

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

under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

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

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

under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

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

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

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

3.4. Intellectual Property Matters

(a) Third Party Claims

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

(b) Contributor APIs

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

(c) Representations.

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

3.5. Required Notices.

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

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

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

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

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

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

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

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

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

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

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

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

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

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

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

<http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____
_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

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

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are Copyright (C) 1998-1999 Netscape Communications Corporation. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the NPL, indicate your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [____]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[____] License."

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

Info-ZIP license

This is version 2007-Mar-4 of the Info-ZIP license.

The definitive version of this document should be available at

<ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely and

a copy at <http://www.info-zip.org/pub/infozip/license.html>.

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LZMA SDK 4.43

OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY O

SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

PCRE 7.4

Copyright (C) 1997-2008, University of Cambridge

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service, Cambridge, England.

Copyright (c) 1997-2007 University of Cambridge

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

ZLIB 1.2

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

OUTILS DE DÉVELOPPEMENT

Informations sur les outils de développement et autres moyens employés par les éditeurs tiers pour créer l'application.

AUTOCONF 2.61

Copyright (C) 1992, 1993, 1994, 1998, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

AUTOMAKE 1.10

Copyright (C) 1994, 1995, 1996, 1997, 1998, 2001, 2003, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

AWK 3.1.5

Copyright (C) 1986, 1988, 1989, 1991-2005, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

BASH 3.2.33

Copyright (C) 1989-2005, Free Software Foundation, Inc

 Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 3 of the License

GCC 4.1.2

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software Foundation, Inc

 Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.4.5

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, Free Software Foundation, Inc

 Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.3.6

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Free Software Foundation, Inc

 Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.3.2

Copyright (C) 1999, 2000, 2001, Free Software Foundation, Inc

 Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GNU MAKE 3.81

Copyright (C) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software

Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

GREP 2.5.1

Copyright 1992, 1997-1999, 2000, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

PERL 5.8.8

Copyright (C) 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Larry Wall and others

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 1 of the License

=====

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:
 - a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
 - b) use the modified Package only within your corporation or organization.
 - c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
 - d) make other distribution arrangements with the Copyright Holder.
4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
 - a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
 - b) accompany the distribution with the machine-readable source of the Package with your modifications.
 - c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
 - d) make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.
6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.
7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.
8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.
9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

SED 4.1.5

Copyright (C)1989, 1990, 1991, 1992, 1993, 1994, 1995, 1998, 1999, 2002, 2003, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

INFORMATIONS DIVERSES

Informations complémentaires sur le code tiers

L'analyse de la signature numérique s'opère à l'aide de la bibliothèque logicielle de protection des données " Agava-S ", développée par OOO " R-Alpha ".

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel.

GNU GENERAL PUBLIC LICENSE

=====

GNU GENERAL PUBLIC LICENSE

Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.

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

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

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies. By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price. Specifically, the General Public License is designed to make sure that you have the freedom to give away or sell copies of free software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

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

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program. You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

- a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and
- b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.
- d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

- a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,
- b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,
- c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

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

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

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

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

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

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

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

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

Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

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

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

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

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (a program to direct compilers to make passes at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

That's all there is to it!

=====

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

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

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

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

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

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

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

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

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

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

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

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

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

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

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

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of

software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

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

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

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

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

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

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

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

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

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

=====

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

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

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

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

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects

or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

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

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

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

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

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

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

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

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

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

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

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type `show c' for details.

The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

=====

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

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

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

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

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

Preamble

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

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

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

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

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

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

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

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

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

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

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

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

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

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

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

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

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

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

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

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

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

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

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

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

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

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

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

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

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

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

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

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

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

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

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

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either

version 2.1 of the License, or (at your option) any later version.

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

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

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

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

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

=====

INDEX

K

KASPERSKY LAB 124

P

Protection antivirus 21