Kaspersky Anti-Virus 8.0 for Lotus Domino

Guide de deploiement

APPLICATION VERSION: 8.0 MAINTENANCE PACK 2

Chers utilisateurs !

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

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

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

Date d'édition : 21/04/2014

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

TABLE DES MATIERES

PRESENTATION DU MANUEL

Ce document constitue le Guide de déploiement de Kaspersky Anti-Virus 8.0 for Lotus® Domino® (ci-après Kaspersky Anti-Virus).

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

Les informations relatives à l'utilisation de l'application, à la configuration des paramètres et à l'administration de la protection d'un serveur ou d'un groupe de serveurs sont détaillées dans le Manuel de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino.

Ce guide est conçu dans les buts suivants :

- Fournir une description générale du fonctionnement de Kaspersky Anti-Virus, des configurations système requises, des scénarios type de déploiement et des particularités de l'intégration aux autres applications.
- Aider à la planification du déploiement de Kaspersky Anti-Virus sur le réseau de l'entreprise.
- Décrire les préparatifs de l'installation de Kaspersky Anti-Virus, et l'installation et l'activation de l'application.
- Prodiguer des conseils sur l'assistance et l'administration de Kaspersky Anti-Virus après l'installation.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes d'obtention du support technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Le Guide de déploiement de Kaspersky Anti-Virus 8.0 for Lotus Domino comporte les sections suivantes :

Sources d'informations sur l'application

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

Kaspersky Anti-Virus 8.0 for Lotus Domino (cf. page 10)

Cette section énumère les principales fonctions de Kaspersky Anti-Virus 8.0 for Lotus Domino.

Configurations matérielle et logicielle requises (cf. page 12)

Cette section présente les configurations matérielle et logicielle minimales requises pour l'installation et le bon fonctionnement de Kaspersky Anti-Virus.

Architecture de l'application (cf. page 15)

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

Administration des privilèges des utilisateurs (cf. page 24)

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

Schémas typiques de déploiement de l'application (cf. page 28)

Cette section décrit les schémas typiques de déploiement de Kaspersky Anti-Virus.

Déploiement de l'application (cf. page 30)

Cette section fournit les informations suivantes :

- description des étapes de déploiement dans le cadre d'un schéma de distribué ou d'un schéma isolé ;
- description de la procédure à suivre avant d'installer Kaspersky Anti-Virus et de commencer à utiliser l'application ;
- instructions d'installation et de suppression de Kaspersky Anti-Virus ;
- informations sur les modifications que l'installation de l'application introduit dans le système.

Contacter le Service de Support Technique (cf. page 51)

Cette section répertorie les recommandations pour contacter le service de support technique de Kaspersky Lab.

Glossaire

Cette section fournit la définition des termes utilisés dans ce document.

Kaspersky Lab ZAO (cf. page 55)

Cette section fournit des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (cf. page 56)

Cette section fournit des informations sur le code tiers utilisé dans l'application.

Notifications sur les marques de commerce

Cette section reprend les marques des tiers qui figurent dans le document.

Index

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

CONVENTIONS

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

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

Tableau 1. Conventions

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

SOURCES D'INFORMATIONS SUR L'APPLICATION

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

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

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

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

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

Si vous n'avez pas trouvé la solution à votre problème, nous vous conseillons de contacter le Support Technique de Kaspersky Lab (cf. section "Support Technique par téléphone" à la page 51).

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

Page du site de Kaspersky Lab

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

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

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

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

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

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

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

Aide électronique

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

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

Documentation

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

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

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

CONTACTER LE SERVICE COMMERCIAL

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

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

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

Ce service est offert en russe et en anglais.

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

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

KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO

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

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

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

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

- Notification des administrateurs sur les objets dangereux découverts lors de l'analyse des documents répliqués et des documents des bases de données, ainsi que sur les actions auxquelles ils sont soumis.

- Enregistrement des objets analysés dans la base de données Quarantaine. Cette action permet de classer par type (messagerie / réplication / analyse des bases de données) les messages et les documents enregistrés qui ont été découverts lors de l'analyse des réplications, ainsi que les documents découverts lors de l'analyse des bases de données.

- Enregistrement des informations sur les objets infectés, potentiellement infectés, protégés et non analysés, ainsi que sur les actions auxquelles ils sont soumis. Ces informations sont enregistrées dans la base de données Journal des événements et statistiques, et s'affichent dans la console du serveur Lotus Domino. Elles peuvent également être enregistrées dans un fichier texte (option désactivée par défaut).

- Mise à jour des bases antivirus via Internet, en mode automatique ou manuel. Les sources de mise à jour des bases peuvent être les serveurs HTTP ou FTP de mise à jour de Kaspersky Lab sur Internet, des serveurs HTTP ou FTP contenant l'ensemble des mises à jour ou des répertoires de réseau.

- Administration des paramètres de fonctionnement de Kaspersky Anti-Virus installé sur plusieurs serveurs grâce aux profils.

- Restriction de l'accès à la configuration des paramètres et à l'administration de Kaspersky Anti-Virus au niveau des serveurs et au niveau des profils.

- Administration du fonctionnement de Kaspersky Anti-Virus via le client Lotus Notes, la console du serveur Lotus Domino et le navigateur.

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

CONFIGURATIONS LOGICIELLE ET MATERIELLE

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

Configurations matérielles :

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

Configurations logicielles :

Systèmes d'exploitation compatibles :

Plateformes 32 bits :

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

Plateformes 64 bits :

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

Versions prises en charge de serveurs Lotus :

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

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

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

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

Navigateurs compatibles :

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

ARCHITECTURE DE L'APPLICATION

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

DANS CETTE SECTION

PRESENTATION DES MODULES FONCTIONNELS DE KASPERSKY ANTI-VIRUS

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

Module d'administration

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

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

Module d'analyse de la messagerie et des copies

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

Module d'analyse des bases de données

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

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

PRESENTATION DES BASES DE DONNEES DE KASPERSKY ANTI-VIRUS

L'application contient les bases de données suivantes :

- Base de données Centre d'administration (kavcontrolcenter.nsf) : elle sert à administrer les paramètres de Kaspersky Anti-Virus et à les enregistrer ;
- Base de données Quarantaine (kavquarantine.nsf) : elle sert à conserver les objets placés en quarantaine et à les manipuler ;
- Base de données Journal des événements et statistiques (kaveventslog.nsf) : elle sert à conserver les entrées sur les événements survenus pendant l'utilisation de Kaspersky Anti-Virus ainsi que les données statistiques concernant les résultats de l'analyse des objets et les actions exécutées sur ceux-ci ;
- Base de données Aide (kavhelp.nsf) : contient l'aide sur l'utilisation de Kaspersky Anti-Virus.

L'accès aux bases citées s'opère via l'interface utilisateur de la base de données Centre d'administration.

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

SCHEMA DE LA PROTECTION ANTIVIRUS DU SERVEUR

Kaspersky Anti-Virus assure la protection de la messagerie et des réplications, et analyse les bases de données conservées sur le serveur. La protection du serveur est assurée par les composants suivants : protection du courrier, protection des réplications et analyse des bases de données (cf. ill. ci-dessous).

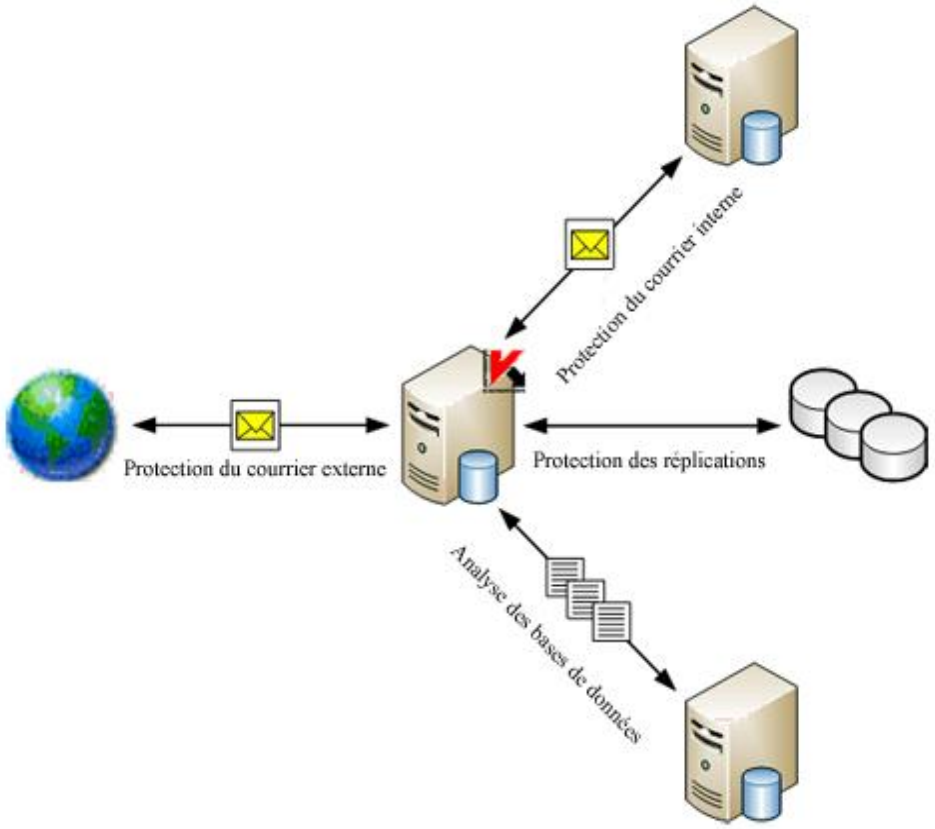

Illustration 1. Schéma de la protection antivirus du serveur Lotus Domino

DANS CETTE SECTION

SCHEMA DE FONCTIONNEMENT DE L'APPLICATION

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

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

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

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

   b. Le filtrage des objets joints (cf. section "Algorithme de filtrage des pièces jointes" à la page 17) selon la taille et (ou) le nom est réalisé.

   c. L'analyse antivirus des objets (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 18) est exécutée.

   d. Les objets sains sont ignorés sans modification tandis que les autres sont traités conformément aux paramètres de la protection (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 19). Avant de passer au traitement, il est possible de conserver une copie de l'objet dans la base de données Quarantaine.

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

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

ALGORITHME DE FILTRAGE DES PIECES JOINTES

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

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

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

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

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

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

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

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

Suite au filtrage, l'objet est traité conformément à l'état attribué par le filtre : l'objet est soumis aux actions (cf. section "Traitement des objets et actions exécutées sur ceux-ci" à la page 19) définies pour les objets de cet état dans les paramètres de la protection du courrier, de la protection des réplications et de l'analyse des bases de données.

ALGORITHME DE LA RECHERCHE D'EVENTUELLES MENACES DANS LES OBJETS

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

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

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

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

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

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

TRAITEMENT DES OBJETS ET ACTIONS EXECUTEES SUR CEUX-CI

Kaspersky Anti-Virus traite les objets conformément à l'état attribué suite au filtrage des pièces jointes (cf. section "Algorithme de filtrage des pièces jointes" à la page 17) et suite à l'analyse antivirus (cf. section "Algorithme de la recherche d'éventuelles menaces dans les objets" à la page 18). Les objets sains sont transmis sans aucune modification aux bases de données du serveur Lotus Domino (modules de protection des réplications et analyse des bases de données) ou au système de messagerie du serveur Lotus Domino (module de protection du courrier). Les actions suivantes peuvent être exécutées sur les objets restants :

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

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

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

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

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

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

Kaspersky Anti-Virus peut prévenir les administrateurs, ainsi que l'expéditeur et les destinataires du message (protection du courrier) de la découverte d'objets et des actions exécutées sur ceux-ci.

ADMINISTRATION DES PARAMETRES DE KASPERSKY ANTI-VIRUS

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

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

Les profils permettent de définir des paramètres uniques de Kaspersky Anti-Virus pour un groupe de serveurs, par exemple sur la base de l'emplacement, des fonctions exécutées ou d'autres facteurs. Cette fonctionnalité simplifie considérablement l'administration de l'application quand elle est installée sur plusieurs serveurs et permet de contrôler de manière centralisée l'état de la protection antivirus sur tous les ordinateurs (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

Le profil peut contenir un ou plusieurs serveurs. En cas d'utilisation d'un schéma isolé de déploiement de Kaspersky Anti-Virus (cf. section "Présentation du déploiement de l'application selon un schéma isolé" à la page 29), seul un serveur entre dans la composition du profil. En cas d'utilisation d'un schéma distribué de déploiement de Kaspersky Anti-Virus (cf. section "Présentation du déploiement de l'application selon un schéma distribué" à la page 28), plusieurs serveurs entrent dans la composition du profil.

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 distinct, dans les paramètres de celui-ci. En outre, il est possible de redéfinir certains paramètres du profil dans les paramètres du serveur. Cette possibilité permet de définir, pour chaque serveur, des paramètres qui correspondent au rôle du serveur dans le système de la protection antivirus et qui diffèrent des valeurs définies dans le profil. Ces paramètres reprennent par exemple les paramètres de mise à jour, les paramètres d'enregistrement des informations sur les événements survenus pendant l'utilisation de Kaspersky Anti-Virus et les informations statistiques.

Les serveurs sont ajoutés automatiquement au profil après l'installation sur ceux-ci de Kaspersky Anti-Virus. En cas de la suppression de l'application, le serveur est automatiquement effacé du profil. Seuls les serveurs protégés par Kaspersky Anti-Virus entrent dans la composition du profil.

Vous pouvez créer et supprimer des profils. Vous pouvez déplacer le serveur sur lequel Kaspersky Anti-Virus est installé d'un profil vers un autre.

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.

Grâce aux paramètres du serveur, vous pouvez configurer les valeurs individuelles correspondant aux fonctions de ce serveur dans le réseau de l'entreprise. Par exemple, les paramètres du serveur peuvent intervenir dans la configuration de la mise à jour centralisée des bases antivirus.

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

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

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

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

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

Les autorisations d'ouverture de la base de données kavcontrolcenter.nsf, de configuration des paramètres et d'administration de Kaspersky Anti-Virus sont octroyées uniquement aux utilisateurs possédant les privilèges 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 nécessaires pour l'exécution des opérations requises (création ou suppression de profils, configuration des paramètres du profil et configuration des paramètres du serveur, etc.).

La base de données kavcontrolcenter.nsf peut être ouverte sur n'importe quel serveur protégé via le client Lotus Notes ou via le navigateur Internet (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

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

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

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

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

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

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

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

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

Tableau 2. Liste des paramètres modifiables

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

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

CONFIGURATION DES PARAMETRES DE SECURITE DU SERVEUR DOMINO

Pour garantir un fonctionnement, une installation et une suppression sans heurt de Kaspersky Anti-Virus, il est nécessaire de configurer les paramètres de sécurité du serveur Lotus Domino. Pour ce faire, utilisez les paramètres indiqués dans l'onglet **Sécurité** (**Security**) du document du serveur, dans le Carnet d'adresses du serveur Lotus Domino (cf. tableau ci-dessous).

Tableau 3. Configuration des paramètres de sécurité du serveur Lotus Domino

PARAMETRES DE PROTECTION	INSTALLATION	CYCLE DE TRAVAIL	SUPPRESSION
Full Remote Console Administrators	Envoi des instructions de la console au serveur des installations primaire et secondaire.	Envoi des instructions de la console à chaque serveur qui utilise une réplique générale de la base de données Centre d'administration.	Redémarrage automatique du serveur Lotus Domino avant la suppression des données de service.
Create Databases & Templates	Création de la base de données des modèles par le serveur, à l'aide duquel le dessin technique de la base de données de l'installation de Kaspersky Anti-Virus a été signé.	Non requis.	Non requis.
Create New Replicas	Création de répliques de bases de données par le serveur des installations primaire et secondaire.	Non requis.	Non requis.

PARAMETRES DE PROTECTION	INSTALLATION	CYCLE DE TRAVAIL	SUPPRESSION
Run Unrestricted Methods and Operations	Les agents en arrière-plan utilisent les instructions de fonctionnement du système de fichiers du serveur : création de répertoire, consultation du contenu des répertoires, appel d'applications externes du côté du serveur, utilisation du contenu de champs RichText.	Les agents en arrière-plan utilisent les instructions de fonctionnement du système de fichiers du serveur : création de répertoire, consultation du contenu des répertoires, appel d'applications externes du côté du serveur, utilisation du contenu de champs RichText.	Les agents en arrière-plan utilisent les instructions de fonctionnement du système de fichiers du serveur : création de répertoire, consultation du contenu des répertoires, appel d'applications externes du côté du serveur.
Trusted Servers	Appel des agents en arrière-plan du serveur de l'installation secondaire à la base de données du serveur de l'installation primaire.	Appel émis par les agents en arrière-plan du serveur vers la base de données de n'importe quel autre serveur utilisant la réplique générale de la base de données Centre d'administration.	Appel de l'agent de la base de données de l'installation de Kaspersky Anti-Virus du serveur de l'installation secondaire à la base de données de Centre d'Administration du serveur de l'installation primaire.

ADMINISTRATION DES PRIVILEGES DES UTILISATEURS

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

L'administration des privilèges des utilisateurs s'opère au niveau de la LCA des bases de données de Kaspersky Anti-Virus et au niveau de chaque document (paramètres du profil et paramètres du serveur). Les privilèges au niveau de la LCA sont octroyés à l'aide du mécanisme des *groupes fonctionnels* (cf. section "*Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus.*" à la page 24). Les privilèges au niveau des documents sont octroyés à l'aide des *rôles fonctionnels* (cf. section "*Administration des privilèges au niveau des paramètres du profil/serveur*" à la page 26).

DANS CETTE SECTION

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

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

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

La LCA des bases de données de Kaspersky Anti-Virus reprend également l'entrée Default (par défaut) et Anonymous (anonyme) ainsi que les serveurs sur lesquels l'application est installée. L'administrateur désigne les serveurs à inclure à la LCA pendant l'installation de l'application (cf. section "Etape 3. Configuration des paramètres de l'installation" à la page 40). 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).

PRIVILEGES DES GROUPES FONCTIONNELS

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

Tableau 4. Privilèges des groupes fonctionnels

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

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

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

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

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

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

Les utilisateurs repris dans le groupe **Administrateurs avec des privilèges restreints** ne possèdent pas, par défaut, les privilèges de modification des paramètres des profils/des serveurs, ni les privilèges de suppression des entrées des bases de données Quarantaine et Journal des événements et statistiques. Les privilèges requis pour l'utilisation de l'application sont octroyés aux utilisateurs de ce groupe à l'aide des rôles fonctionnels (cf. section "Administration des privilèges au niveau des paramètres du profil/du serveur" à la page 26).

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

OCTROI DE PRIVILEGES DES GROUPES FONCTIONNELS AUX UTILISATEURS

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

Pour simplifier la procédure d'octroi des privilèges, il est conseillé de ne pas inclure des utilisateurs individuels dans les groupes fonctionnels, mais bien les groupes composés dans le carnet d'adresses du serveur Lotus Domino (cf. section "Constitution de groupes d'utilisateurs pour l'octroi des privilèges" à la page 35). Pendant l'installation, ces groupes sont inclus dans la LCA des bases de données de Kaspersky Anti-Virus et ils reçoivent les privilèges des groupes fonctionnels (cf. section "Privilèges des groupes fonctionnels" à la page 24). Plus tard, l'administrateur du serveur Lotus Domino pourra octroyer aux utilisateurs des privilèges ou les restreindre en modifiant la composition des groupes dans le carnet d'adresses (exclusion ou inclusion d'utilisateurs).

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

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

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

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

1. Créez, dans le carnet d'adresses du serveur Lotus Domino, un groupe portant un nom unique, par exemple ControlCenterAdmins.
2. Ajoutez l'utilisateur qui recevra les privilèges de tel ou tel groupe fonctionnel, par exemple du groupe **Administrateurs du centre d'administration**, au groupe ControlCenterAdmins.
3. Ouvrez une session dans le système sous le compte de l'utilisateur possédant les privilèges du groupe fonctionnel **Administrateur de la sécurité**.
4. Ajoutez le groupe ControlCenterAdmins à la LCA des bases de données de Kaspersky Anti-Virus (Centre d'administration, Journal des événements et statistiques, Quarantaine et Aide) et définissez pour le groupe ControlCenterAdmins les privilèges qui correspondent aux privilèges du groupe fonctionnel **Administrateur du Centre d'administration** (cf. section "**Privilèges des groupes fonctionnels**" à la page 24).

ADMINISTRATION DES PRIVILEGES AU NIVEAU DES PARAMETRES DU PROFIL/SERVEUR

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

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

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

Les administrateurs de profil et les administrateurs de serveur sont désignés après l'installation de l'application. La désignation a lieu pour chaque serveur et chaque profil séparément.

Seul un utilisateur possédant les privilèges de l'un des trois groupes fonctionnels peut être désigné comme administrateur de profil ou administrateur de serveur.

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

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

SCHEMAS DE DEPLOIEMENT TYPIQUES DE L'APPLICATION

Cette section décrit les schémas typiques de déploiement de Kaspersky Anti-Virus. Vous pouvez déployer Kaspersky Anti-Virus sur le réseau de l'entreprise, soit selon un schéma distribué, soit selon un schéma isolé.

DANS CETTE SECTION

PRESENTATION DU DEPLOIEMENT DE L'APPLICATION SELON UN SCHEMA DISTRIBUE

Le déploiement de Kaspersky Anti-Virus selon un schéma distribué implique l'installation de l'application sur plusieurs serveurs Lotus Domino. Dans ce cas, toutes les instances installées de Kaspersky Anti-Virus représentent un seul système distribué. Il est recommandé d'utiliser un schéma distribué de déploiement dans les situations suivantes :

- Le réseau de l'entreprise présente plusieurs serveurs Lotus Domino, y compris dans les clusters. Dans ce cas, Kaspersky Anti-Virus doit être installé sur chaque serveur.

  La configuration d'un serveur avec partitions (Partitioned) n'est pas prise en charge.

- Le réseau de l'entreprise présente une connexion permanente entre les serveurs Lotus Domino.
- Le trafic réseau n'est pas limité ni en termes de volumes de données transférées, ni en ce qui concerne la vitesse de transfert des données.
- Le répertoire des bases de données du serveur Lotus Domino est relié à des disques présentant suffisamment d'espace libre.

Grâce au déploiement de Kaspersky Anti-Virus selon un schéma distribué, il vous est possible d'exécuter les actions suivantes :

- centraliser l'administration des paramètres de protection et des tâches principales de Kaspersky Anti-Virus sur l'ensemble des serveurs Lotus Domino protégés (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino) ;
- obtenir un accès à la configuration des paramètres de l'application et aux bases de données Journal des événements et statistiques et Quarantaine à partir de n'importe quel serveur Lotus Domino ;
- administrer les paramètres de protection et les privilèges des groupes fonctionnels d'utilisateurs au niveau des groupes de serveurs ;
- adapter automatiquement la configuration du réseau de l'entreprise lors de l'ajout d'un nouveau serveur Lotus Domino protégé dans le schéma distribué ou lors de la suppression d'un serveur de ce schéma.

L'installation de Kaspersky Anti-Virus s'effectue indépendamment sur chaque serveur du réseau de l'entreprise. Pour commencer, il faut réaliser *installation primaire* de l'application. Le serveur sur lequel l'application est installée en premier est appelé *serveur de l'installation primaire*. Ensuite, Kaspersky Anti-Virus est installé sur l'ensemble des *serveurs complémentaires*.

Si la réplication dans le réseau Lotus Domino adopte une topologie en étoile, il est conseillé de choisir le serveur central du réseau (hub) en tant que serveur de l'installation primaire.

Les bases de données de Kaspersky Anti-Virus sont créées sur le serveur de l'installation primaire. Après l'installation sur les serveurs complémentaires, la configuration de l'application et les bases de données sont reproduites successivement sur les autres serveurs. Lors de l'installation sur chaque serveur complémentaire suivant, l'un des serveurs sur lequel Kaspersky Anti-Virus est déjà installé peut être désigné en tant que serveur de l'installation primaire.

Il est conseillé de placer une seule réplique des bases de données Kaspersky Anti-Virus sur chaque serveur Lotus Domino protégé. Cela permet d'éviter les conflits d'administration de l'application et la perte de données.

Kaspersky Anti-Virus peut être installé de l'une des deux manières suivantes : via un client Lotus Notes ou via un navigateur Internet. La séquence à suivre pour l'installation de l'application ne dépend pas du mode d'installation choisi, ni du système d'exploitation du serveur Lotus Domino. Ceci étant dit, les étapes des préparatifs pour l'installation (cf. section "Préparatifs pour l'installation" à la page 32) et des préparatifs pour l'utilisation (cf. section "Préparatifs pour l'utilisation" à la page 46) sont réalisées différemment en fonction du mode d'installation de l'application.

La tâche HTTP doit être lancée afin d'assurer la réussite de l'installation à distance de l'application via le navigateur Internet sur le serveur Lotus Domino qui servira de référence pour cette même installation sur les autres serveurs.

PRESENTATION DU DEPLOIEMENT DE L'APPLICATION SELON UN SCHEMA ISOLE

Lors du déploiement de Kaspersky Anti-Virus selon un schéma isolé, l'installation de l'application s'effectue indépendamment sur plusieurs serveurs Lotus Domino. Il est recommandé d'utiliser un schéma de déploiement isolé dans les situations suivantes :

- Le réseau de l'entreprise ne présente pas de connexion permanente entre les serveurs Lotus Domino.
- Le trafic réseau est limité en termes de volumes de données transférées et de vitesse de transfert des données.
- Le répertoire des bases de données du serveur Lotus Domino est relié à des disques présentant peu d'espace libre.

Lors du déploiement de Kaspersky Anti-Virus selon un schéma isolé, l'installation primaire de l'application (cf. section "Configuration des paramètres de l'installation primaire" à la page. 40) s'exécute séparément sur chaque serveur du réseau de l'entreprise. Le serveur doit posséder les privilèges nécessaires (cf. section "Configuration des privilèges du serveur de l'installation" à la page 34).

Kaspersky Anti-Virus peut être installé de l'une des deux manières suivantes : via un client Lotus Notes ou via un navigateur Internet. La séquence à suivre pour l'installation de l'application ne dépend pas du mode d'installation choisi, ni du système d'exploitation du serveur Lotus Domino. Ceci étant dit, les étapes des préparatifs pour l'installation (cf. section "Préparatifs pour l'installation" à la page 32) et des préparatifs pour l'utilisation (cf. section "Préparatifs pour l'utilisation" à la page 46) sont réalisées différemment en fonction du mode d'installation de l'application.

La tâche HTTP doit être lancée afin d'assurer la réussite de l'installation à distance de l'application via le navigateur Internet sur le serveur Lotus Domino qui servira de référence pour cette même installation sur les autres serveurs.

DEPLOIEMENT DE L'APPLICATION

Cette section fournit les informations suivantes :

- description des étapes de déploiement dans le cadre d'un schéma de distribué ou d'un schéma isolé ;
- description de la procédure à suivre avant d'installer Kaspersky Anti-Virus et de commencer à utiliser l'application ;
- instructions d'installation et de suppression de Kaspersky Anti-Virus ;
- informations sur les modifications que l'installation de l'application introduit dans le système.

DANS CETTE SECTION

ETAPES DU DEPLOIEMENT DE L'APPLICATION SELON UN SCHEMA DISTRIBUE

Le déploiement de Kaspersky Anti-Virus selon un schéma distribué contient les étapes suivantes :

1. **Préparatifs pour l'installation**. Avant d'installer Kaspersky Anti-Virus, il convient de réaliser les opérations suivantes :

   - Supprimer la version antérieure de Kaspersky Anti-Virus et toute autre application antivirus pour Lotus Notes/Domino de chaque serveur sur lequel Kaspersky Anti-Virus 8.0 sera installé (cf. section "Suppression de la version antérieure de Kaspersky Anti-Virus et d'autres applications antivirus pour Lotus Notes/Domino' à la page 33).
   - Définir les privilèges de l'utilisateur qui réalisera l'installation (cf. section "Configuration des privilèges de l'utilisateur qui réalisera l'installation de Kaspersky Anti-Virus" à la page 33).
   - Définir, dans le carnet d'adresses du serveur de l'installation primaire, le groupe de serveurs sur lesquels Kaspersky Anti-Virus sera installé (cf. section "Création du groupe de serveurs d'installation dans le carnet d'adresses" à la page 34).
   - Configurer les privilèges pour chaque serveur sur lequel l'application sera installée (cf. section "Configuration des privilèges de l'installation" à la page 34).

- Créer, dans le carnet d'adresses, les groupes d'utilisateurs Lotus Domino qui disposeront des privilèges des groupes fonctionnels pour l'utilisation de l'application (cf. section "Création de groupes d'utilisateurs pour l'octroi des privilèges" à la page 35).
- Placer la base de données d'installation dans le répertoire de données de chaque serveur Lotus Domino où l'application sera installée.
- Vérifier l'intégrité de la base de données d'installation (cf. section "Vérification de l'intégrité de la base de données d'installation" à la page 36).
- Signer la base de données d'installation (cf. section "Préparation de la base de données d'installation" à la page 36).
- Configurer les paramètres de sécurité sur les postes de travail si l'installation de Kaspersky Anti-Virus est exécutée via un client Lotus Notes (cf. section "Configuration des paramètres de sécurité du client Lotus Notes" à la page 36).

2. **Installation de l'application sur le serveur de l'installation primaire** (cf. section "**Configuration des paramètres de l'installation primaire**" à la page 40).
3. **Installation de l'application sur un serveur complémentaire**. L'installation s'exécute successivement sur chaque serveur complémentaire (cf. section "Configuration des paramètres de l'installation primaire" à la page 40).

Le serveur de l'installation primaire doit être accessible au serveur complémentaire.

4. **Préparatifs pour l'utilisation**. Avant de commencer à utiliser Kaspersky Anti-Virus, il est nécessaire de réaliser les opérations suivantes :
   - Configurer les paramètres de sécurité pour chaque poste de travail d'où sera utilisé Kaspersky Anti-Virus (cf. section "Préparatifs pour l'utilisation" à la page 46).
   - Activer l'application sur chaque serveur doté de Kaspersky Anti-Virus si elle n'avait pas été activée au moment de son installation (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

ETAPES DU DEPLOIEMENT DE L'APPLICATION SELON UN SCHEMA ISOLE

Le déploiement de Kaspersky Anti-Virus selon un schéma isolé se décompose ainsi :

1. **Préparatifs pour l'installation**. Avant d'installer Kaspersky Anti-Virus, il convient de réaliser les opérations suivantes :
   - Supprimer la version antérieure de Kaspersky Anti-Virus et toute autre application antivirus pour Lotus Notes/Domino de chaque serveur sur lequel Kaspersky Anti-Virus 8.0 sera installé (cf. section "Suppression de la version antérieure de Kaspersky Anti-Virus et d'autres applications antivirus pour Lotus Notes/Domino' à la page 33).
   - Définir les privilèges de l'utilisateur qui réalisera l'installation (cf. section "Configuration des privilèges de l'utilisateur qui réalisera l'installation de Kaspersky Anti-Virus" à la page 33).
   - Créer, dans le carnet d'adresses, le groupe de serveurs sur lesquels Kaspersky Anti-Virus sera installé (cf. section "Création du groupe de serveurs d'installation dans le carnet d'adresses" à la page 34).
   - Configurer les privilèges pour chaque serveur sur lequel l'application sera installée (cf. section "Configuration des privilèges de l'installation" à la page 34).

- Créer, dans le carnet d'adresses des serveurs d'installation, les groupes d'utilisateurs Lotus Domino qui disposeront des privilèges des groupes fonctionnels pour l'utilisation de l'application (cf. section "Création de groupes d'utilisateurs pour l'octroi des privilèges" à la page 35).
- Placer la base de données d'installation dans le répertoire de données de chaque serveur Lotus Domino où l'application sera installée.
- Vérifier l'intégrité de la base de données d'installation (cf. section "Vérification de l'intégrité de la base de données d'installation" à la page 36).
- Signer la base de données d'installation (cf. section "Préparation de la base de données d'installation" à la page 36).
- Configurer les paramètres de sécurité sur les postes de travail si l'installation de Kaspersky Anti-Virus est exécutée via un client Lotus Notes (cf. section "Configuration des paramètres de sécurité du client Lotus Notes" à la page 36).

2. **Installation primaire sur le serveur**. L'installation s'exécute successivement sur tous les serveurs où Kaspersky Anti-Virus doit être installé (cf. section "Configuration des paramètres de l'installation primaire" à la page 40).
3. **Préparatifs pour l'utilisation**. Avant de commencer à utiliser Kaspersky Anti-Virus, il est nécessaire de réaliser les opérations suivantes :
   - Configurer les paramètres de sécurité pour chaque poste de travail d'où sera utilisé Kaspersky Anti-Virus (cf. section "Préparatifs pour l'utilisation" à la page 46).
   - Activer l'application sur chaque serveur doté de Kaspersky Anti-Virus si elle n'avait pas été activée au moment de son installation (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

PREPARATIFS POUR L'INSTALLATION

Cette section détaille les actions à réaliser avant d'installer Kaspersky Anti-Virus.

Avant de lancer l'installation, assurez-vous que l'ordinateur répond à la configuration logicielle et matérielle requise pour Kaspersky Anti-Virus (cf. section "Configurations logicielles et matérielles requises" à la page 12).

DANS CETTE SECTION

SUPPRESSION DE LA VERSION ANTERIEURE DE KASPERSKY ANTI-VIRUS ET D'AUTRES LOGICIELS ANTIVIRUS POUR LOTUS NOTES/DOMINO

Kaspersky Anti-Virus 8.0 for Lotus Domino n'est pas compatible avec d'autres logiciels antivirus pour Lotus Notes/Domino. L'utilisation conjointe de Kaspersky Anti-Virus et d'autres logiciels antivirus pourrait entraîner des situations anormales.

Si d'autres logiciels antivirus pour Lotus Notes/Domino ou une version antérieure de Kaspersky Anti-Virus sont installés, il est conseillé de les supprimer avant d'installer Kaspersky Anti-Virus 8.0 for Lotus Domino.

La mise à jour des versions antérieures de Kaspersky Anti-Virus for Lotus Domino jusqu'à la version 8.0 n'est pas prise en charge.

CONFIGURATION DES PRIVILEGES DE L'UTILISATEUR QUI INSTALLERA KASPERSKY ANTI-VIRUS

L'utilisateur qui installe Kaspersky Anti-Virus doit posséder les privilèges nécessaires à l'exécution des opérations suivantes dans la LCA de la base de données d'installation du serveur Lotus Domino :

- accès au Carnet d'adresses principal du serveur Lotus Domino au moins au niveau Editor (Editeur), avec la possibilité de modifier les documents du serveur et de créer et de modifier les groupes ;
- utilisation des méthodes et des opérations sans restriction (Sign or run unrestricted methodes and operations) ;
- utilisation de la console distante Lotus Domino (Full remote console administrators) ;
- création de bases de données et de modèles de base de données (Create databases & templates) ;
- création de répliques de bases de données (Create new replicas).

Avant d'installer l'application, assurez-vous que votre compte utilisateur possède les privilèges requis.

Par défaut, la LCA de la base de données d'installation reprend les enregistrements Default (par défaut) avec le niveau d'accès No access (pas d'accès) et le groupe LocalDomainAdmins avec le niveau d'accès Manager (gestionnaire) et les privilèges de création, de suppression ou de copie de documents. Si le groupe LocalDomainAdmins ne figure pas sur le serveur d'installation ou si l'utilisateur qui installe Kaspersky Anti-virus n'appartient pas à ce groupe, il est nécessaire de modifier la LCA de la base de données d'installation avant de lancer l'installation.

Il est impossible d'intégrer un utilisateur Anonymous dans la LCA et de lui attribuer les privilèges sur la base de données d'installation qui sont indispensables à l'installation de l'application. L'utilisateur du compte Anonymous ne possède pas les privilèges de collecte des informations indispensables à la configuration. Ainsi, l'installation de l'application se soldera par une erreur. Il est primordial que l'installation de l'application soit réalisée au nom de l'administrateur possédant les privilèges requis.

➡ *Pour configurer les privilèges de l'utilisateur qui installera Kaspersky Anti-Virus,*

ajoutez son compte à la LCA de la base d'installation directement ou dans un groupe, et octroyez-lui le niveau d'accès Manager (gestionnaire) et les privilèges de création, de suppression, de réplication ou de copie de documents.

CREATION DU GROUPE DE SERVEURS D'INSTALLATION DANS LE CARNET D'ADRESSES

Au cours de l'installation primaire de Kaspersky Anti-Virus, vous devez indiquer les serveurs sur lesquels l'application sera installée (cf. section "Configuration des paramètres de l'installation primaire" à la page 40). Les serveurs indiqués seront automatiquement repris dans la LCA des bases de données de Kaspersky Anti-Virus. Les serveurs d'installation reçoivent dans la LCA le niveau d'accès Manager (gestionnaire) auquel sont associées les autorisations de création, de suppression de réplication ou de copie de documents.

Si le déploiement de Kaspersky Anti-Virus s'exécute selon le schéma distribué, il est nécessaire d'indiquer tous les serveurs sur lesquels Kaspersky Anti-Virus doit être installé lors de l'installation de l'application sur le serveur d'installation primaire. Les serveurs supplémentaires qui ne sont pas indiqués lors de l'installation primaire doivent être ajoutés manuellement dans la LCA de toutes les bases de données de Kaspersky Anti-Virus.

Pour simplifier la procédure d'octroi des privilèges, il est conseillé, pendant l'installation, de ne pas désigner des serveurs individuels d'installation, mais des groupes de serveurs dans le carnet d'adresses. Pour cela, avant de lancer l'installation, créez dans le carnet d'adresses un groupe de serveurs (par exemple KavProtectedServers) et ajoutez-y tous les serveurs sur lesquels il est prévu d'installer Kaspersky Anti-Virus. Plus tard, vous pourrez administrer les privilèges des serveurs en modifiant la composition de ce groupe dans le carnet d'adresses.

Si les serveurs d'installation n'étaient pas repris dans un groupe et qu'un serveur supplémentaire quelconque n'a pas été ajouté à la LCA lors de l'installation primaire, il convient de procéder de la manière suivante pour lui octroyer les privilèges :

1. Créer dans le carnet d'adresses du serveur Domino un groupe portant un nom unique, par exemple KavProtectedServers.
2. Ajouter au groupe KavProtectedServers le serveur qui doit recevoir les privilèges.
3. Entrer dans le système avec le compte utilisateur de la personne inscrite dans le groupe fonctionnel **Administrateurs de la sécurité** (cf. section "**Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus.**" à la page 24).

   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.

4. Ajouter le groupe KavProtectedServers dans la LCA des bases de données de Kaspersky Anti-Virus (bases de données Centre d'administration, Journal des événements et statistiques, Quarantaine) et définir, pour le groupe KavProtectedServers, les privilèges qui correspondent aux privilèges du serveur d'installation : niveau d'accès Manager (gestionnaire) avec privilèges de création, de suppression, de réplication et de copie de documents.

Si, à l'Etape 3. Configuration des paramètres de l'installation primaire (cf. section "Configuration des paramètres de l'installation primaire" à la page 40), dans le groupe **Paramètres de déploiement**, la case **Conserver les objets de la quarantaine dans toutes les répliques** est cochée, le groupe de serveurs ajoutés doit se voir attribuer le rôle AllAccessible dans la LCA de la base de données Quarantaine. Si ce rôle n'est pas attribué, chaque réplique de la base de données Quarantaine conserve uniquement les objets de son propre serveur.

CONFIGURATION DES PRIVILEGES DU SERVEUR D'INSTALLATION

Chaque serveur sur lequel Kaspersky Anti-Virus est installé doit disposer des privilèges suivants :

- Utiliser la console distante de Lotus Domino (Full remote console administrators).
- Utiliser les méthodes et les opérations sans restriction (Sign or run unrestricted methodes and operations).
- Créer de bases de données et des modèles de base de données (Create databases & templates).
- Créer des répliques de bases de données (Create new replicas).

De plus, si le déploiement de l'application s'exécute selon un schéma distribué, tous les serveurs sur lesquels Kaspersky Anti-Virus est installé doivent figurer dans la liste des serveurs de confiance (Trusted Servers) de chaque serveur.

La configuration des paramètres de sécurité des serveurs s'exécute sous l'onglet **Sécurité** (Security) du document du serveur, dans le Carnet d'adresses du serveur Lotus Domino.

Pour administrer les privilèges des serveurs, il est conseillé d'utiliser un groupe de serveurs d'installation créé dans le carnet d'adresses (cf. section "Création du groupe de serveurs d'installation dans le carnet d'adresses" à la page 34).

Après l'installation de Kaspersky Anti-Virus sur tous les serveurs, vous pouvez retirer les privilèges suivants au serveur d'installation :

- création de bases de données et de modèles de base de données (Create databases & templates) ;
- création de répliques de bases de données (Create new replicas).

Les privilèges suivants ne sont pas nécessaires au bon fonctionnement de Kaspersky Anti-Virus.

CREATION DE GROUPES D'UTILISATEURS POUR L'OCTROI DES PRIVILEGES

L'octroi aux utilisateurs des privilèges requis pour l'utilisation de Kaspersky Anti-Virus s'opère en incluant les utilisateurs dans des groupes fonctionnels : **Administrateurs de la sécurité**, **Administrateurs du centre d'administration** et **Administrateurs avec des privilèges restreints** (cf. section "**Administration des privilèges des utilisateurs au niveau des LCA des bases de données de Kaspersky Anti-Virus**" à la page 24). La composition de chacun de ces groupes est définie lors de l'installation de l'application.

Les groupes fonctionnels sont composés uniquement lors de l'installation primaire de Kaspersky Anti-Virus. La LCA des bases de données du serveur d'installation primaire est utilisée en tant que source d'informations sur la composition des groupes fonctionnels lors de l'installation de l'application sur les serveurs complémentaires, dans le cadre d'un schéma de déploiement distribué.

Afin de simplifier la procédure d'octroi de privilèges, il est conseillé d'inclure dans les groupes fonctionnels non pas des utilisateurs distincts, mais des groupes d'utilisateurs du carnet d'adresses du serveur Lotus Domino. Avant de commencer l'installation, créez des groupes d'utilisateurs dans le Carnet d'adresse Lotus Domino. Ces groupes seront utilisés pour l'attribution des privilèges. Le nom du groupe peut être quelconque. Vous pouvez créer les groupes suivants :

- **SecurityAdmins** : groupe qui figurera dans le groupe fonctionnel **Administrateurs de la sécurité** ;
- **ControlCenterAdmins** : groupe qui figurera dans le groupe fonctionnel **Administrateurs du centre d'administration** ;
- **RestrictedAdmins** : groupe qui figurera dans le groupe fonctionnel **Administrateurs avec des privilèges restreints**.

La composition de chaque groupe fonctionnel est déterminée au cours de l'installation de l'application sur le serveur de l'installation primaire (cf. section "Configuration des paramètres de l'installation primaire" à la page 40).

Au moment d'installer Kaspersky Anti-Virus, les groupes d'utilisateurs qui recevront les privilèges des groupes fonctionnels **Administrateurs du centre d'administration** et **Administrateur avec des privilèges restreints** peuvent être vides. Des utilisateurs pourront y être ajoutés après l'installation de l'application. Le groupe d'utilisateurs qui va recevoir les privilèges du groupe fonctionnel **Administrateurs de la sécurité** doit contenir au moins un utilisateur du carnet d'adresses.

VERIFICATION DE L'INTEGRITE DES BASES DE DONNEES D'INSTALLATION

Pour vérifier l'intégrité de la base de données d'installation, procédez comme suit :

1. Ouvrez la console du serveur Lotus Domino.
2. Dans la ligne de commande, saisissez l'instruction `Load fixup kavinstaller.nsf`.

Une fois que l'intégrité de la base de données d'installation a été vérifiée, il est nécessaire de préparer cette dernière (cf. section "Vérification de l'intégrité de la base de données d'installation" à la page 36).

PREPARATION DE LA BASE DE DONNEES D'INSTALLATION

Le fichier d'installation de l'application est un fichier de base de données Lotus Notes.

Avant de lancer l'installation de Kaspersky Anti-Virus, placez la base de données d'installation dans le répertoire de données du serveur sur lequel l'installation a lieu et signez-la à l'aide du compte utilisateur du serveur qui possède les privilèges nécessaires (cf. section "Configuration des privilèges du serveur" à la page 34).

Il est conseillé de signer la base d'installation à l'aide du compte utilisateur du serveur sur lequel l'installation a lieu.

En cas d'installation de l'application sur plusieurs serveurs, cette base de données d'installation signée doit être installée sur chaque serveur.

Lors de l'installation de Kaspersky Anti-Virus sur un serveur complémentaire, vous pouvez utiliser la base d'installation déjà signée avant le début de l'installation de l'application sur le serveur d'installation primaire. Copiez-la depuis le répertoire de données du serveur de l'installation primaire.

Il est nécessaire de vérifier l'intégrité de la base de données d'installation avant de la signer (cf. section "Vérification de l'intégrité de la base de données d'installation" à la page 36).

Suite à la vérification de l'intégrité de la base de données et à sa signature, il convient de relancer le serveur Lotus Domino.

VERIFICATION DE LA DISPONIBILITE DU FICHIER CLE

Si vous possédez un fichier clé, vous pourrez activer Kaspersky Anti-Virus au moment de l'installation.

Pour pouvoir activer la licence pendant l'installation de l'application, assurez-vous que le fichier clé est accessible via le système de fichiers de l'ordinateur client à partir duquel la base de données d'installation est ouverte.

Si vous ne disposez pas d'un fichier clé au moment de l'installation, vous pourrez activer l'application après son installation via l'interface de la console du serveur Lotus Domino, via le client Lotus Notes ou via le navigateur Internet (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

CONFIGURATION DES PARAMETRES DE SECURITE DU CLIENT LOTUS NOTES

Si l'installation de Kaspersky Anti-Virus est réalisée via le client Lotus Notes, il est nécessaire de configurer au préalable la table d'administration des actions sur le poste de travail qui sera utilisé pour se connecter au serveur.

Octroyez au compte utilisateur utilisé pour signer la base de données d'installation les autorisations suivantes d'accès et d'exécution d'opérations sur ce poste de travail (cf. ill. ci-dessous) :

- **Autorisations d'accès** :
  - au système de fichiers (File system) ;
  - à l'application externe (External code) ;
  - à la base de données Lotus Notes actuelle (Current database) ;
  - aux variables d'environnement (Environment variables) ;
  - aux applications externes (External programs) ;
  - aux bases de données autres que Lotus Notes (Non-Notes databases).
- **Autorisations** :
  - envoi du courrier (Send mail) ;
  - lecture d'autres bases de données que Notes (Read other databases) ;
  - exportation de données (Export data) ;
  - modification d'autres bases de données que Notes (Read other databases).

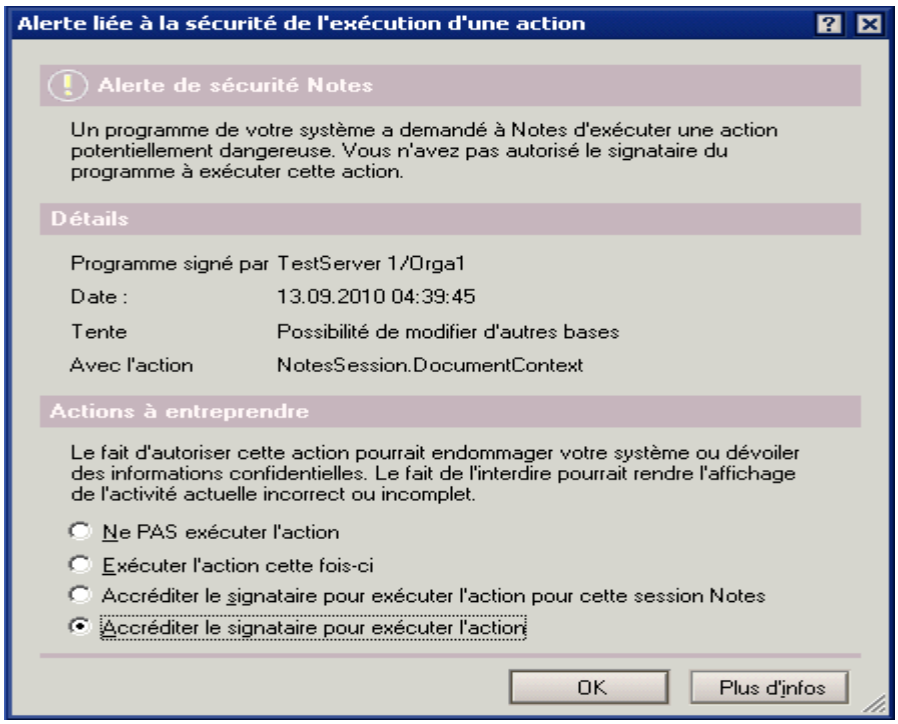

Illustration 2. Configuration des paramètres de sécurité du client Lotus Notes

INSTALLATION DE L'APPLICATION

Cette section explique comment installer l'application sur l'ordinateur. Les procédures d'installation de l'application sur le serveur d'installation primaire et d'installation sur un serveur complémentaire sont identiques pour la majeure partie (cf. tableau ci-dessous). Quand les étapes diffèrent, les actions propres à chaque type d'installation sont décrites séparément dans les sous-rubriques de l'étape d'installation correspondante.

Tableau 5. Etapes de l'installation primaire de l'application et de l'installation sur un serveur complémentaire

INSTALLATION PRIMAIRE DE L'APPLICATION	INSTALLATION DE L'APPLICATION SUR UN SERVEUR COMPLEMENTAIRE
1. Début de l'installation.	
2. Acceptation du contrat de licence.	
3. Configuration des paramètres d'installation de l'application sur le serveur d'installation primaire.	3. Configuration des paramètres de l'installation de l'application sur un serveur complémentaire.
4. Lancement et exécution de l'installation. a. Vérification des paramètres de l'installation. b. Création des bases de données. c. Création de la configuration. d. Copie des fichiers de service. e. Génération des variables d'environnement.	4. Lancement et exécution de l'installation. a. Vérification des paramètres de l'installation. b. Création de la configuration. c. Création des bases de données. d. Copie des fichiers de service. e. Génération des variables d'environnement.
5. Activation de la licence (l'étape peut être ignorée si vous ne possédez pas de fichier clé).	
6. Fin de l'installation.	

DANS CETTE SECTION

ÉTAPE 1. DEBUT DE L'INSTALLATION

Avant de lancer l'installation, assurez-vous que le compte de l'utilisateur qui installera Kaspersky Anti-Virus possède tous les privilèges requis (cf. section "Configuration des privilèges de l'utilisateur qui réalisera l'installation" à la page 33). Lors de l'installation de l'application, l'authentification de l'utilisateur est obligatoire. Si l'authentification n'est pas activée, l'application ne sera pas installée.

Kaspersky Anti-Virus peut être installé via le client Lotus Notes ou via le navigateur Internet.

➧ *Pour lancer l'installation de Kaspersky Anti-Virus via le client Lotus Notes, procédez comme suit :*

1. Lancez le client Lotus Notes.
2. Ouvrez la base de données d'installation située dans le répertoire de données du serveur d'installation.

Pour lancer l'installation de Kaspersky Anti-Virus via le navigateur Internet, procédez comme suit :

1. Ouvrez le navigateur Internet.
2. Saisissez, dans la ligne d'adresse :

   `http://<nom_du_serveur>/<chemin_de_la_base_de_données_d'installation>?OpenDatabase&Login`

   où :

   - `<nom_du_serveur>` est le nom ou l'adresse IP du serveur où Kaspersky Anti-Virus est installé ;
   - `<chemin_de_la_base_de_données_d'installation>` est le chemin d'accès à la base de données d'installation relatif au répertoire des données du serveur d'installation.

Cette action entraîne l'ouverture de la fenêtre de l'Assistant d'installation. Le reste des opérations de l'installation de l'application aura lieu dans cette fenêtre.

Si Kaspersky Anti-Virus n'a jamais été installé sur le serveur, la fenêtre de l'Assistant d'installation affiche le texte du Contrat de licence (cf. section "Etape 2. Acceptation du contrat de licence" à la page 39).

Si le serveur est déjà doté d'une version antérieure de Kaspersky Anti-Virus, la fenêtre de l'Assistant affiche les informations sur le système ainsi que le bouton **Supprimer**. Pour installer Kaspersky Anti-Virus 8.0 for Lotus Domino, il est nécessaire de supprimer la version déjà installée de l'application (cf. section "Suppression de Kaspersky Anti-Virus" à la page 47).

ÉTAPE 2. ACCEPTATION DU CONTRAT DE LICENCE

Lisez le texte du contrat de licence dans la fenêtre de l'Assistant d'installation. Vous devez accepter les conditions du Contrat de licence pour poursuivre l'installation de l'application.

Pour marquer votre accord sur les conditions du Contrat de licence,

cliquez sur le bouton **Accepter**.

Une fois que vous avez accepté les conditions du Contrat de licence, la fenêtre de l'Assistant d'installation affiche les informations suivantes :

- Informations sur le système.
- Paramètres de déploiement.
- Sécurité.
- Répertoires d'installation de Kaspersky Anti-Virus.
- Liste des étapes automatiques de l'installation de l'application.

Pour lancer l'exécution automatique des étapes de l'installation de l'application en utilisant les paramètres par défaut,

cliquez sur le bouton **Continuer**.

Pour interrompre l'installation de l'application,

cliquez sur le bouton **Quitter**.

ÉTAPE 3. CONFIGURATION DES PARAMETRES DE L'INSTALLATION

Configurez les paramètres de l'installation. Par défaut, Kaspersky Anti-Virus propose d'exécuter l'installation de l'application sur le serveur de l'installation primaire (cf. section "Schémas typiques de déploiement de l'application" à la page 28).

CONFIGURATION DES PARAMETRES DE L'INSTALLATION PRIMAIRE

Pour configurer les paramètres de l'installation primaire de Kaspersky Anti-Virus, procédez comme suit :

1. Assurez-vous que la case **Installation primaire** est cochée dans le groupe **Paramètres de déploiement**.

2. Choisissez un mode d'enregistrement des objets dans la base de données Quarantaine et ses répliques. Pour ce faire, dans le groupe **Paramètres de déploiement**, cochez la case **Enregistrer les objets en quarantaine dans toutes les répliques**:

   - Quand la case est cochée, la base de données Quarantaine conserve les objets de son serveur et de tous les autres serveurs inclus dans la configuration distribuée. La valeur **Enregistrer les objets en quarantaine dans toutes les répliques** apparaît dans le groupe **Informations sur le système**.

   Tous les serveurs de la configuration distribuée doivent se voir attribuer un rôle AllAccessible dans la LCA de la base de données Quarantaine (cf. section "Création du groupe de serveurs d'installation dans le carnet d'adresses" à la page 34).

   - Si la case **Enregistrer les objets en quarantaine dans toutes les répliques** est décochée, les répliques de la base de données Quarantaine conservent uniquement les objets de leur propre serveur. La valeur **Les répliques de la quarantaine contiennent uniquement les objets de son serveur** apparaît dans le groupe **Informations sur le système**.

3. Indiquez le groupe de serveurs sur lesquels il est prévu d'installer Kaspersky Anti-Virus dans le champ **Serveurs protégés** du groupe **Sécurité**.

   Vous pouvez saisir le nom de groupes de serveurs ou le nom de serveurs individuels. Pour simplifier la procédure d'administration des privilèges, il est conseillé d'utiliser des groupes de serveurs d'installation du Carnet d'adresses (cf. section "Création du groupe de serveurs d'installation dans le carnet d'adresses" à la page 34). Cliquez sur le bouton à droite du champ de saisie et sélectionnez le groupe de serveurs du Carnet d'adresses du serveur Lotus Domino, ou saisissez manuellement le nom du groupe. Vous pouvez indiquer un ou plusieurs groupes dans chaque champ.

   Le champ **Serveurs protégés** reprend par défaut le groupe **LocalDomainServers**.

4. Indiquez les groupes d'utilisateurs Lotus Domino qui seront repris dans les groupes fonctionnels du même nom dans les champs **Administrateurs de la sécurité**, **Administrateurs du centre d'administration** et **Administrateurs avec des privilèges restreints**.

   Vous pouvez saisir le nom de groupes d'utilisateurs ou le nom d'utilisateurs individuels. Pour simplifier la procédure d'administration des privilèges, il est conseillé d'utiliser des groupes d'utilisateurs (cf. section "Création de groupes d'utilisateurs pour l'octroi des privilèges" à la page 35). Cliquez sur le bouton à droite du champ de saisie et sélectionnez le groupe d'utilisateurs dans le Carnet d'adresses du serveur Lotus Domino, ou saisissez manuellement le nom du groupe. Vous pouvez indiquer un ou plusieurs groupes dans chaque champ.

   Le groupe **LocalDomainAdmins** est repris par défaut dans les champs **Administrateurs de la sécurité**, **Administrateurs du Centre d'administration** et **Administrateurs avec des privilèges restreints**.

5. Saisissez le chemin d'accès au répertoire du serveur où seront installées les bases de données Lotus Notes de Kaspersky Anti-Virus dans le champ **Répertoire des bases de données** du groupe **Répertoires d'installation de Kaspersky Anti-Virus**. Le chemin indiqué par défaut dans le champ est celui de kavdatabases.

CONFIGURATION DES PARAMETRES DE L'INSTALLATION SUR UN SERVEUR COMPLEMENTAIRE

Pour configurer les paramètres d'installation de Kaspersky Anti-Virus sur un serveur complémentaire, procédez comme suit :

1. Dans le groupe **Paramètres de déploiement**, décochez la case **Installation primaire**. La liste des groupes de la fenêtre de l'Assistant d'installation est modifiée.

2. Indiquez le serveur sur lequel l'application est déjà installée dans le champ **Serveur de l'installation primaire** du groupe **Paramètres de déploiement**. Les bases de données de Kaspersky Anti-Virus seront répliquées depuis ce serveur sur le serveur supplémentaire. Pour ce faire, cliquez sur le bouton à droite du champ de saisie et sélectionnez le serveur dans le Carnet d'adresses du serveur Domino, ou saisissez manuellement le nom du serveur.

3. Dans le champ **Répertoire des bases de données du serveur d'installation primaire**, saisissez le chemin d'accès au répertoire sur le serveur d'installation primaire qui héberge les bases de données Lotus Notes de Kaspersky Anti-Virus. Le chemin d'accès est relatif au répertoire des données du serveur Domino. Le chemin indiqué par défaut dans le champ est celui de kavdatabases.

4. Saisissez le chemin d'accès au répertoire du serveur où seront installées les bases de données Lotus Notes de Kaspersky Anti-Virus dans le champ **Répertoire des bases de données** du groupe **Répertoires d'installation de Kaspersky Anti-Virus**. Le chemin indiqué par défaut dans le champ est celui de kavdatabases.

ÉTAPE 4. LANCEMENT ET EXECUTION DES ETAPES AUTOMATIQUES DE L'INSTALLATION

A ce stade, l'Assistant d'installation de Kaspersky Anti-Virus exécute automatiquement l'installation de l'application en quelques étapes. Les étapes diffèrent entre l'installation primaire (cf. section "Exécution des étapes automatiques de l'installation primaire" à la page 42) et l'installation sur un serveur complémentaire (cf. section "Exécution des étapes automatiques de l'installation sur un serveur complémentaire" à la page 43). La liste des étapes apparaît dans la partie inférieure de la fenêtre de l'Assistant d'installation.

Vérifiez minutieusement les paramètres d'installation avant de lancer l'exécution automatique des étapes de l'installation (cf. section "Etape 3. Configuration des paramètres de l'installation" à la page 40).

Pour lancer l'exécution des étapes automatiques de l'installation,

cliquez sur le bouton **Continuer**.

L'icône apparaît à côté du nom de chaque étape de l'installation si elle a réussi. En cas d'échec, c'est l'icône qui apparaît. Dès que étape exécutée a réussi, l'Assistant d'installation passe à l'étape suivante.

Si l'étape s'est soldée sur une erreur, l'installation est interrompue. Dans ce cas, vérifiez que toutes les étapes de préparation ont bien été exécutées, puis recommencez l'étape. En cas d'erreur, vous pouvez également contacter le Service de Support Technique (cf. page 51).

Pour interrompre l'installation de l'application,

cliquez sur le bouton **Quitter**.

Les informations relatives aux événements enregistrés lors de l'installation sont consignées dans le journal d'installation (kavsetuplog.nsf) et dans le journal des événements du serveur Lotus Domino. Elles apparaissent également sur la console du serveur et à l'écran, sous la forme de notifications.

EXECUTION DES ETAPES AUTOMATIQUES DE L'INSTALLATION PRIMAIRE

Les étapes automatiques de l'installation primaire sont réalisées dans l'ordre suivant :

1. Vérification des paramètres de l'installation.

   Cette étape correspond à la vérification de l'exactitude des paramètres d'installation primaire (cf. section "Configuration des paramètres de l'installation primaire" à la page 40).

2. Création des bases de données.

   Cette étape correspond à la création des bases de données suivantes dans le répertoire des bases de données de Kaspersky Anti-Virus :

   - Journal d'installation (kavsetuplog.nsf).
   - Centre d'administration (kavcontrolcenter.nsf).
   - Journal des événements et statistiques (kaveventslog.nsf).
   - Quarantaine (kavquarantine.nsf).
   - Aide (kavhelp.nsf).
   - Base de données de service de Kaspersky Anti-Virus (kavlocale.nsf).

   Chaque base de données est signée par un compte utilisateur du serveur sur lequel l'installation a lieu.

   Une liste des enregistrements pour le contrôle de l'accès (LCA) est créée pour chaque base de données directement après sa création. La constitution de la LCA repose sur les groupes d'utilisateurs et de serveurs désignés lors de la configuration des paramètres de l'installation primaire (cf. section "Configuration des paramètres de l'installation primaire" à la page 40).

   > Les groupes d'utilisateurs et de serveurs sont formés lors des Préparatifs de l'installation (cf. section "Préparatifs pour l'installation" à la page 32).

   La LCA reprend également les entrées Default et Anonymous. Le niveau d'accès No Access (pas d'accès) leur est attribué.

3. Création de la configuration.

   Cette étape correspond à la composition, dans la base de données Centre d'administration, du profil auquel sera ajouté le serveur protégé.

4. Copie des fichiers de service.

   Cette étape correspond au déploiement des bibliothèques, des fichiers exécutables et de la sélection initiale des bases antivirus.

5. Génération des variables d'environnement.

   Cette étape correspond à la configuration automatique du chemin d'accès aux bases Lotus Notes de Kaspersky Anti-Virus et du chemin d'accès aux fichiers exécutables.

Si toutes les étapes automatisées de l'installation de Kaspersky Anti-Virus réussissent, le message **L'installation a réussi** s'affiche dans la partie inférieure de la fenêtre de l'Assistant d'installation.

EXECUTION DES ETAPES AUTOMATIQUES DE L'INSTALLATION SUR UN SERVEUR COMPLEMENTAIRE

Les étapes automatiques de l'installation sur un serveur supplémentaire sont exécutées dans l'ordre suivant :

1. Vérification des paramètres de l'installation.

   Cette étape correspond à la vérification de l'exactitude des paramètres pour l'installation sur un serveur complémentaire (cf. section "Configuration des paramètres de l'installation sur un serveur complémentaire" à la page 41).

2. Création de la configuration.

   Cette étape correspond à l'ajout des informations relatives au nouveau serveur dans la base de données Centre d'administration sur le serveur de l'installation primaire. Le nouveau serveur est ajouté au même profil que le serveur de l'installation primaire.

3. Création des bases de données.

   Cette étape correspond à la copie de toutes les bases de données de Kaspersky Anti-Virus, créées lors de l'installation primaire, sur le serveur complémentaire :

   - Journal d'installation (kavsetuplog.nsf).
   - Centre d'administration (kavcontrolcenter.nsf).
   - Journal des événements et statistiques (kaveventslog.nsf).
   - Quarantaine (kavquarantine.nsf).
   - Aide (kavhelp.nsf).
   - Base de données de service de Kaspersky Anti-Virus (kavlocale.nsf).

   Assurez-vous que le processus de création d'une réplique des bases de données sur le serveur complémentaire a réussi. Si ce n'est pas le cas, interrompez la procédure d'installation et recréez les répliques des bases de données sur le serveur complémentaire.

4. Copie des fichiers de service.

   Cette étape correspond au déploiement des bibliothèques, des fichiers exécutables et de la sélection initiale des bases antivirus.

5. Génération des variables d'environnement.

   Cette étape correspond à la configuration automatique du chemin d'accès aux bases Lotus Notes de Kaspersky Anti-Virus et du chemin d'accès aux fichiers exécutables.

Si toutes les étapes automatisées de l'installation de Kaspersky Anti-Virus se terminent avec succès, le message **L'installation a réussi** s'affiche dans la partie inférieure de la fenêtre de l'Assistant d'installation.

FIN DES ETAPES AUTOMATISEES D'INSTALLATION

Une fois la dernière étape d'installation automatisée **Génération des variables d'environnement** terminée, les boutons **Activation de l'application** et **Redémarrer le serveur** apparaissent dans la fenêtre de l'Assistant d'installation.

Vous pouvez passer à l'Etape 5. Activation de l'application (cf. section "Etape 5. Activation de l'application" à la page 44) à l'aide du bouton **Activation de l'application** ou ignorer cette étape et passer directement à l'Etape 6. Fin de l'installation (cf. section "Etape 6. Fin de l'installation" à la page 44) à l'aide du bouton **Redémarrer le serveur**. Dans ce cas, l'installation sera réalisée sans l'activation.

ÉTAPE 5. ACTIVATION DE L'APPLICATION

Le fichier clé doit être accessible via le système de fichiers de l'ordinateur client d'où la base de données d'installation est ouverte.

Pour activer l'application, procédez comme suit :

1. Cliquez sur le bouton **Activation de l'application** dans la fenêtre de l'Assistant d'installation.
2. Dans la fenêtre qui s'ouvre, sélectionnez le fichier clé, puis cliquez sur le bouton **Ouvrir**.

Le fichier clé sera appliqué de façon automatique et un message apparaîtra à l'écran pour confirmer l'activation de l'application. Vous pouvez ensuite fermer la fenêtre de sélection du fichier clé et passer à l'étape suivante de l'installation (cf. section "Etape 6. Fin de l'installation" à la page 44).

Si vous ne disposez pas d'un fichier clé au moment de l'installation de Kaspersky Anti-Virus, vous pouvez ignorer cette étape d'installation et activer l'application ultérieurement via l'interface de la console du serveur Lotus Domino, via le client Lotus Notes ou via le navigateur Internet (informations détaillées dans le Manuel de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

ÉTAPE 6. FIN DE L'INSTALLATION

Pour terminer l'installation, il est nécessaire de redémarrer le serveur Lotus Domino. Cliquez sur le bouton **Redémarrer le serveur** pour procéder au redémarrage.

Dans le cadre de l'installation de l'application sur un serveur complémentaire, assurez-vous que la procédure de réplication des bases de données de Kaspersky Anti-Virus a réussi avant de redémarrer le serveur.

Pour terminer l'installation de Kaspersky Anti-Virus,

cliquez sur le bouton **Redémarrer le serveur** dans la fenêtre de l'Assistant d'installation.

La fenêtre de l'Assistant d'installation se ferme. Le serveur Lotus Domino redémarre.

MODIFICATIONS DANS LE SYSTEME APRES L'INSTALLATION

Cette section détaille les modifications apportées au système après l'installation de Kaspersky Anti-Virus. Les modifications suivantes sont introduites dans le système :

- des fichiers et des répertoires sont créés ;
- le fichier de configuration Lotus Domino (notes.ini) est modifié ;
- liste des processus est modifiée.

DANS CETTE SECTION

FICHIERS ET REPERTOIRES DE L'APPLICATION

Les répertoires suivants sont créés sur le serveur Lotus Domino à l'issue de l'installation de l'application Kaspersky Anti-Virus :

- kavcommon : répertoire de service de Kaspersky Anti-Virus. Le répertoire est créé à l'emplacement suivant :
  - pour les systèmes d'exploitation Microsoft Windows : dans le répertoire des fichiers binaires Lotus Domino (par défaut : C:\Program Files\Lotus\Domino) ;
  - Pour les systèmes d'exploitation Linux : dans le répertoire des données du serveur Lotus Domino (par défaut : /local/notesdata).
- Répertoire des bases de données de Kaspersky Anti-Virus, désigné par l'utilisateur lors de l'installation de l'application (cf. section "Etape 3. Configuration des paramètres de l'installation" à la page 40). Par défaut, le répertoire kavdatabases constitue le répertoire de stockage des bases de données. Il est créé à l'emplacement suivant :
  - pour les systèmes d'exploitation Microsoft Windows : dans le répertoire de données du serveur Lotus Domino (par défaut : C:\Program Files\Lotus\Domino\Data) ;
  - Pour les systèmes d'exploitation Linux : dans le répertoire des données du serveur Lotus Domino (par défaut : /local/notesdata).

Les bases de données suivantes sont créées dans le répertoire kavdatabases des bases de données de Kaspersky Anti-Virus :

- kavsetuplog.nsf (Journal d'installation) ;
- kavcontrolcenter.nsf (Centre d'administration) ;
- kaveventslog.nsf (Journal des événements et statistiques) ;
- kavquarantine.nsf (Quarantaine) ;
- kavhelp.nsf (Aide) ;
- kavlocale.nsf (base de données de service de Kaspersky Anti-Virus).

MODIFICATIONS APPORTEES AU FICHIER DE CONFIGURATION LOTUS DOMINO

Les modifications suivantes sont introduites dans le fichier de configuration Lotus Domino (notes.ini) après l'installation de l'application :

- Le nom de la tâche `KAVControl` pour l'exécution automatique de la tâche au démarrage du serveur Lotus Domino est ajouté à la variable de base `ServerTasks` ;
- La ligne suivante est ajoutée à la variable de base `EXTMGR_ADDINS`. Il s'agit des noms des bibliothèques assurant l'interception des documents :
  - pour les systèmes d'exploitation Microsoft Windows, il s'agit de la ligne `kavlhook` ;
  - pour les systèmes d'exploitation Linux, il s'agit de la ligne `<chemin_complet_vers_le_répertoire_de_données_Domino>/libnklhook.so`.
- La valeur `ASCII Text,2,_XTEXT,,.C,.H,.PRN,.RIP,.TXT,._UNKNOWN,,1` qui garantit les transformations requises des champs de type Rich Text pour l'analyse suivante est définie dans la variable de base `EDITEXP1`.

- La variable `KAVDatabasesPath` qui permet de désigner le chemin d'accès aux bases de données Lotus Notes de Kaspersky Anti-Virus est créée.
- La variable `KAVNonIncrementalScan=1` qui désactive l'analyse incrémentale est créée.
- La variable `KAVProcExclude` qui indique les processus d'exclusion de l'analyse de Kaspersky Anti-Virus est créée. Les valeurs `updall, nupdate, ldap, event, statlog, fixup, compact` sont attribuées à la variable.
- La variable `KAVArchDepthLevel=32` qui détermine le niveau d'imbrication autorisé par défaut pour les archives est créée.

MODIFICATION DANS LA LISTE DE PROCESSUS

Les processus suivants sont ajoutés à la liste des processus suite à l'installation de Kaspersky Anti-Virus :

- `KAVControl` : module d'administration.
- `KAVMonitor` : module d'analyse du courrier et des copies.
- `KAVScanner` : module d'analyse des bases de données.

PREPARATIFS POUR L'UTILISATION

Kaspersky Anti-Virus démarre automatiquement au lancement du serveur Lotus Domino. La protection antivirus est active dès le lancement de Kaspersky Anti-Virus. Les modules KAVControl, KAVMonitor, KAVScanner sont ajoutés à la liste des processus chargés.

Avant d'utiliser Kaspersky Anti-Virus, il est nécessaire d'activer l'application sur chaque serveur si cela n'a pas été fait au moment de son installation (informations détaillées dans le Manuel de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino). Tant que l'application n'est pas activée, ses fonctionnalités sont limitées.

Une tentative de mise à jour automatique des bases antivirus est lancée à la première exécution de l'application. Les paramètres de mise à jour par défaut sont utilisés (par exemple, le lancement de la première mise à jour des bases antivirus a lieu à 23 h 00 ou après l'activation de l'application). Si la configuration du réseau diffère de la configuration par défaut, alors la mise à jour se solde sur une erreur. Le message d'erreur est enregistré dans la base de données Journal des événements et statistiques.

Si la mise à jour des bases antivirus s'est soldée sur une erreur, il est conseillé de configurer les paramètres de mise à jour et d'exécuter manuellement la mise à jour des bases antivirus (informations détaillées dans le Guide de l'administrateur de Kaspersky Anti-Virus 8.0 for Lotus Domino).

La configuration des paramètres de Kaspersky Anti-Virus et l'administration de son fonctionnement s'opèrent via l'interface de la base de données Centre d'administration (kavcontrolcenter.nsf). La connexion à la base kavcontrolcenter.nsf est réalisée à l'aide des méthodes traditionnelles de Lotus/Domino : via le client Lotus Notes ou via le navigateur Web.

Si les manipulations de la base de données sont réalisées via le client Lotus Notes, il est nécessaire de configurer les paramètres de sécurité du poste de travail utilisé pour se connecter au serveur avant de commencer.

Il n'est pas nécessaire de configurer les paramètres de sécurité sur le poste de travail à partir duquel Kaspersky Anti-Virus a été installé car ceux-ci ont été configurés lors des préparatifs pour l'installation (cf. section "Configuration des paramètres de sécurité du client Lotus Notes" à la page 36).

Pour ce faire, il est nécessaire d'ajouter au tableau d'administration des actions (cf. ill. ci-après) le compte utilisateur du serveur qui a signé les éléments des bases de données Lotus Notes de Kaspersky Anti-Virus et d'octroyer à ce compte les privilèges suivants pour accéder aux actions et les exécuter sur le poste de travail en question :

- **Autorisations d'accès** :
  - au système de fichiers (File system) ;
  - à la base de données Lotus Notes actuelle (Current database) ;
  - aux variables d'environnement (Environment variables) ;
  - aux applications externes (External programs).
- **Autorisations** :
  - lecture d'autres bases de données que Notes (Read other databases) ;
  - modification d'autres bases de données que Notes (Read other databases).

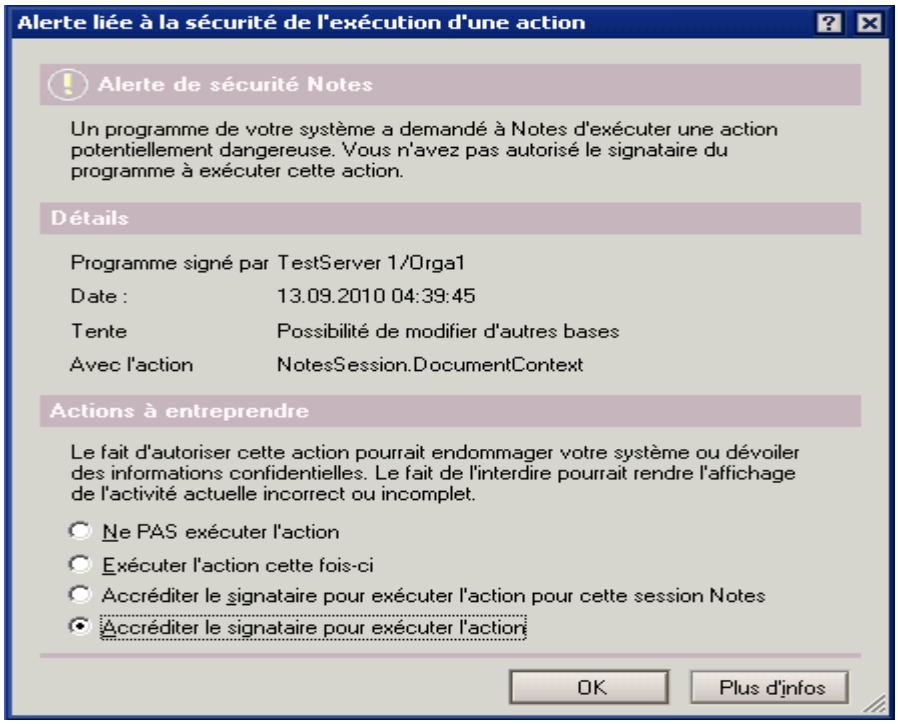

Illustration 3. Configuration des paramètres de sécurité du client Lotus Notes

La configuration des paramètres de sécurité du client Lotus Notes est réalisée sur chaque poste de travail utilisé pour accéder à la base de données Centre d'administration.

SUPPRESSION DE KASPERSKY ANTI-VIRUS

Cette section décrit les actions à exécuter avant la suppression de Kaspersky Anti-Virus. Elle fournit également des instructions pour la suppression de l'application dans le cadre d'un schéma de déploiement distribué ou isolé.

La base de données d'installation permet de supprimer Kaspersky Anti-virus. La suppression de l'application doit être effectuée indépendamment sur chaque serveur.

Si Kaspersky Anti-Virus a été installé selon un schéma isolé, la suppression de l'application sur chaque serveur s'exécute comme sur le dernier serveur du schéma de déploiement distribué (cf. section "Suppression sur le dernier serveur dans le schéma distribué de déploiement" à la page 48).

Dans le cadre d'un schéma distribué de déploiement, il est possible de supprimer Kaspersky Anti-virus sur tous les serveurs où il est installé ou sur certains d'entre eux uniquement.

Pour supprimer Kaspersky Anti-Virus d'un ou de plusieurs serveurs, il est nécessaire, sur chacun de ces serveurs, de supprimer l'application à partir de l'un des serveurs du schéma de déploiement distribué (à la page 49). Si un schéma de déploiement distribué est utilisé et que Kaspersky Anti-Virus est supprimé de l'un des serveurs de ce schéma, les informations relatives à ce serveur sont supprimées des répliques de la base de données Centre d'administration figurant sur les autres serveurs. Après la suppression de Kaspersky Anti-Virus sur un ou plusieurs serveurs, le fonctionnement de l'application sur les autres serveurs ne sera pas perturbé.

Pour supprimer Kaspersky Anti-Virus de tous les serveurs où il est installé, il est nécessaire de le supprimer successivement de chaque serveur de la même manière que sur le dernier serveur dans le schéma distribué de déploiement (cf. section "Suppression sur le dernier serveur dans le schéma distribué de déploiement" à la page 48).

DANS CETTE SECTION

PREPARATIFS POUR LA SUPPRESSION DE KASPERSKY ANTI-VIRUS

Avant de supprimer Kaspersky Anti-Virus, il est nécessaire de réaliser les opérations suivantes :

- placer la base de données d'installation signée dans le répertoire de données du serveur sur lequel l'application doit être supprimée (cf. section "Préparation de la base de données d'installation" à la page 36) ;
- vérifier l'intégrité de la base de données d'installation (cf. section "Vérification de l'intégrité de la base de données d'installation" à la page 36) ;
- vérifier l'exactitude de la configuration des privilèges du serveur (cf. section "Configuration des privilèges du serveur d'installation" à la page 34) et de l'utilisateur qui réalisera la suppression de l'application (cf. section "Configuration des privilèges de l'utilisateur qui réalisera l'installation de Kaspersky Anti-Virus" à la page 33) ;
- si la suppression de l'application est réalisée via le client Lotus Notes, s'assurer que les paramètres de sécurité du client Lotus Notes ont été configurés (cf. section "Configuration des paramètres de sécurité du client Lotus Notes" à la page 36).

SUPPRESSION DE L'APPLICATION SUR LE DERNIER SERVEUR DU SCHEMA DE DEPLOIEMENT DISTRIBUE

Pour supprimer Kaspersky Anti-Virus du dernier serveur dans le schéma distribué de déploiement, procédez comme suit :

1. Ouvrez la base de données d'installation via le client Lotus Notes ou via le navigateur Internet (cf. section "Etape 1. Début de l'installation" à la page 38).

   Cette action entraîne l'ouverture de la fenêtre de l'Assistant de suppression de l'application. La fenêtre de l'Assistant de suppression affiche les informations sur le système, les paramètres de la configuration et la liste des étapes de la suppression de l'application.

2. Vérifiez que la case **Suppression sur le dernier serveur dans la configuration** est cochée dans le groupe **Informations sur le système**.

3. Cliquez sur le bouton **Supprimer**. Confirmez le redémarrage du serveur Lotus Domino dans la fenêtre de saisie.

   Attendez que l'Assistant de suppression exécute la première étape de la suppression de l'application **Génération des variables d'environnement**. Au cours de cette étape, les modifications introduites suite à l'installation de Kaspersky Anti-Virus (cf. section "Modifications dans le fichier de configuration de Lotus Domino" à la page 45) sont automatiquement supprimées du fichier de configuration notes.ini. Une fois la première étape terminée, le serveur Lotus Domino redémarre automatiquement.

4. Après le redémarrage du serveur, cliquez sur le bouton **Supprimer** dans la fenêtre de l'Assistant de suppression de l'application.

   Patientez pendant que l'Assistant de suppression exécute les étapes automatisées suivantes de suppression de l'application. L'icône apparaît à côté du nom de chaque étape si elle a réussi. En cas d'échec, c'est l'icône qui apparaît.

5. À l'issue de toutes les étapes de la suppression, fermez la fenêtre de l'Assistant de suppression de l'application.

Si l'une des étapes automatisées de la suppression de l'application s'est soldée sur une erreur, le processus de suppression de l'application s'interrompt. Dans ce cas, il est nécessaire de fermer la fenêtre de l'Assistant de suppression et de relancer la suppression.

SUPPRESSION DE L'APPLICATION SUR L'UN DES SERVEURS DU SCHEMA DE DEPLOIEMENT DISTRIBUE

Pour supprimer Kaspersky Anti-Virus sur un des serveurs dans le schéma distribué de déploiement, procédez comme suit :

1. Ouvrez la base de données d'installation via le client Lotus Notes ou via le navigateur Internet (cf. section "Etape 1. Début de l'installation" à la page 38).

   Cette action entraîne l'ouverture de la fenêtre de l'Assistant de suppression de l'application. La fenêtre de l'Assistant de suppression affiche les informations sur le système, les paramètres de la configuration et la liste des étapes de la suppression de l'application.

2. Si la suppression a lieu via le client Lotus Notes, décochez la case **Suppression sur le dernier serveur dans la configuration** du groupe **Informations sur le système**. La liste des groupes de la fenêtre de l'Assistant de suppression est modifiée.

3. Indiquez, dans le champ **Serveur de l'installation primaire**, le serveur sur lequel il reste des copies des bases de données de Kaspersky Anti-Virus. Pour ce faire, cliquez sur le bouton à droite du champ de saisie et sélectionnez le serveur dans le Carnet d'adresses du serveur Domino, ou saisissez manuellement le nom du groupe.

4. Saisissez, dans le champ **Répertoire des bases de données du serveur d'installation primaire**, le chemin d'accès au répertoire des bases de données Lotus Notes de Kaspersky Lab sur le serveur sélectionné à l'étape précédente. Le chemin d'accès est relatif au répertoire des données du serveur Domino. Le chemin indiqué par défaut dans le champ est celui de kavdatabases.

5. Cliquez sur le bouton **Supprimer**. Confirmez le redémarrage du serveur Lotus Domino dans la fenêtre de saisie.

   Attendez que l'Assistant de suppression exécute la première étape de la suppression de l'application **Génération des variables d'environnement**. A cette étape, les opérations suivantes s'exécutent automatiquement :

   - les modifications introduites suite à l'installation de Kaspersky Anti-Virus (cf. section "Modifications dans le fichier de configuration de Lotus Domino" à la page 45) sont supprimées du fichier de configuration notes.ini. ;

- les informations relatives au serveur sur lequel Kaspersky Anti-Virus est supprimé seront effacées de la réplique de la base de données Centre d'administration du serveur indiqué à l'Etape 3 de l'installation de l'application (cf. section "Etape 3. Configuration des paramètres d'installation" à la page 40).

Une fois la première étape de suppression terminée, le serveur Lotus Domino redémarre automatiquement.

6. Après le redémarrage du serveur, cliquez sur le bouton **Supprimer** dans la fenêtre de l'Assistant de suppression de l'application.

   Patientez pendant que l'Assistant de suppression exécute les étapes automatisées suivantes de suppression de l'application. L'icône  apparaît à côté du nom de chaque étape si elle a réussi. En cas d'échec, c'est l'icône  qui apparaît.

7. À l'issue de toutes les étapes de la suppression, fermez la fenêtre de l'Assistant de suppression de l'application.

Si l'une des étapes automatisées de la suppression de l'application s'est soldée sur une erreur, le processus de suppression de l'application s'interrompt. Dans ce cas, il est nécessaire de fermer la fenêtre de l'Assistant de suppression et de relancer la suppression.

CONTACTER LE SERVICE DE SUPPORT TECHNIQUE

Cette section présente les différentes méthodes d'obtention du Support Technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Service de Support Technique.

DANS CETTE SECTION

MODES D'OBTENTION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans l'une des sources d'informations relatives à l'application (cf. section "Sources d'informations sur l'application" à la page 8), contactez le Service de Support Technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le Support Technique, veuillez lire les règles d'octroi du Support Technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du Service de Support Technique de l'une des manières suivantes :

- Par téléphone. Vous pouvez contacter les experts du Service de Support Technique en France.
- En envoyant une demande depuis Kaspersky Company Account sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Service Support Technique via un formulaire.

Le support technique est fourni uniquement aux utilisateurs de l'application ayant acheté une licence. Le support technique n'est pas prévu pour les utilisateurs d'une version d'évaluation.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique français http://support.kaspersky.com/fr/b2b.

Avant de contacter le Service de Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique (http://support.kaspersky.com/fr/support/rules). Nos experts pourront ainsi vous venir en aide plus rapidement.

OBTENTION DU SUPPORT TECHNIQUE VIA KASPERSKY COMPANY ACCOUNT

Kaspersky Company Account (https://companyaccount.kaspersky.com) est un service Web conçu pour l'envoi de demandes à Kaspersky Lab et le suivi de leur traitement par les spécialistes.

Pour accéder à Kaspersky Company Account, il vous est demandé de vous inscrire. Vous pouvez vous inscrire seul sur la page d'inscription (https://support.kaspersky.com/companyaccount/registration?LANG=fr) ou par l'intermédiaire d'un utilisateur enregistré disposant des droits d'administrateur sur le compte utilisateur de votre entreprise dans Kaspersky CompanyAccount.

Dans Kaspersky Company Account, le compte utilisateur de votre entreprise est créé dès le premier enregistrement de la licence Kaspersky Company Account acquise par votre société. Tous les employés enregistrés dans Kaspersky Company Account sont associés à ce compte utilisateur.

Si un nouveau compte utilisateur est créé pour votre entreprise lors de l'inscription à Kaspersky CompanyAccount, les privilèges concernant son administration vous sont attribués par défaut. Il s'agit des privilèges couvrant l'ensemble des actions possibles avec ce compte utilisateur. Si, lors de l'inscription, vous vous ajoutez à un compte utilisateur existant, des privilèges restreints vous sont attribués par défaut.

Pour en savoir plus sur Kaspersky Company Account et sur les actions qu'il vous permet de réaliser, consultez la page du site Internet du Support Technique http://support.kaspersky.com/fr/faq/companyaccount_help.

Demande adressée par email au Support Technique

Vous pouvez envoyer une demande par email au Service de Support Technique en anglais, en russe et dans d'autres langues.

Lors de la soumission d'une demande, spécifiez les renseignements suivants :

- type de demande ;
- nom et version de l'application ;
- texte de la demande.

Si nécessaire, vous pouvez également joindre des fichiers au formulaire de demande électronique.

Un spécialiste du Service de Support Technique vous répond via le système Kaspersky Company Account à l'adresse électronique que vous avez indiquée lors de l'inscription.

Demande adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Service de Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivants au laboratoire d'étude des virus :

- si vous suspectez que le fichier ou la ressource Web contient un virus mais que Kaspersky Anti-Virus ne détecte aucune menace. Les experts du laboratoire d'étude des virus analysent le fichier ou l'URL envoyé et, en cas de découverte d'un virus inconnu jusque-là, ils ajoutent les informations le concernant à la base des données accessible lors de la mise à jour des applications antivirus de Kaspersky Lab ;
- si Kaspersky Anti-Virus identifie un fichier ou une ressource Web comme porteur d'un virus mais que vous êtes sûr que ce n'est pas le cas.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus via le formulaire de demande (https://my.kaspersky.com/fr/kpc/newrequest) sans vous enregistrer dans Kaspersky Company Account.

GLOSSAIRE

A

ACTIVATION DE L'APPLICATION

L'application devient entièrement fonctionnelle. L'utilisateur effectue l'activation pendant ou après l'installation de l'application. Pour pouvoir activer l'application, l'utilisateur doit disposer d'un code d'activation ou d'un fichier de clé.

ANALYSEUR HEURISTIQUE

Technologie de détection des menaces dont les définitions ne figurent pas encore dans les bases de Kaspersky Lab. L'analyseur heuristique permet de détecter les objets dont le comportement dans le système opérationnel peut représenter une menace pour la sécurité. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Ainsi, un objet potentiellement infecté peut être un objet qui contient une séquence d'instructions caractéristiques des programmes malveillants (ouverture d'un fichier, écriture dans un fichier).

B

BALAYAGE PROGRESSIF

Analyse sélective des fichiers. Lors du balayage progressif, l'application analyse uniquement les fichiers modifiés depuis la dernière analyse.

BASES ANTIVIRUS

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Ces bases antivirus sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

M

MISE A JOUR DES BASES

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

O

OBJET OLE

Objet rattaché à un autre fichier ou intégré à un autre fichier à l'aide de la technologie Object Linking and Embedding (OLE). Par exemple, un objet OLE peut être un tableau Microsoft Office Excel®, intégré à un document Microsoft Office Word.

OBJET INFECTE

Objet dont un segment de code correspond parfaitement à un segment de code d'une application connue présentant une menace. Les experts de Kaspersky Lab déconseillent l'utilisation de tels objets.

OBJET POTENTIELLEMENT INFECTE.

Objet dont le code contient un extrait modifié de code d'un programme dangereux connu ou objet dont le comportement évoque un tel programme.

Q

QUARANTAINE

Dossier dans lequel l'application de Kaspersky Lab place les objets potentiellement infectés détectés. Les objets en quarantaine sont enregistrés sous forme chiffrée pour éviter toute action de leur part sur l'ordinateur.

R

REPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Il n'est pas possible de réparer tous les objets infectés.

S

SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab à partir desquels les applications de Kaspersky Lab reçoivent les mises à jour des bases et des modules de l'application.

KASPERSKY LAB

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

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

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

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

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

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

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

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

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

Site de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com
Laboratoire d'étude des virus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets potentiellement infectés sous forme d'archive)
	https://my.kaspersky.com/fr/kpc/newrequest
	(pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

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

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Google Chrome est une marque de Google, Inc.

Intel et Pentium sont des marques déposées de Intel Corporation aux Etats-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans d'autres pays.

Lotus, Domino et Lotus Notes sont des marques commerciales d'International Business Machines Corporation enregistrées dans de nombreuses juridictions à travers le monde.

Excel, Internet Explorer, Microsoft, Windows et Windows Server sont des marques déposées de Microsoft Corporation aux Etats-Unis et dans d'autres pays.

Mozilla et Firefox sont des marques de Mozilla Foundation.

Novell est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

Red Hat et Red Hat Enterprise Linux sont des marques commerciales de Red Hat Inc. déposées aux Etats-Unis et dans d'autres pays.

INDEX

S