Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG

Manuel d'installation

VERSION DE L'APPLICATION : 8.5

Chers utilisateurs

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

Ce document peut être modifié sans un avertissement préalable. La version la plus récente du manuel sera disponible sur le site de Kaspersky Lab, à l'adresse suivante : http://www.kaspersky.com/fr/docs.

Date d'édition du document : 18/06/2012

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

TABLE DES MATIERES

PRESENTATION DU MANUEL 5
Dans ce document 5
Conventions 6
SOURCES D'INFORMATIONS SUR L'APPLICATION 8
Sources d'informations pour les recherches indépendantes 8
Discussion sur les logiciels de Kaspersky Lab sur le forum 9
Contacter le service commercial 9
Contacter le Groupe de localisation et de documentation 9
KASPERSKY ANTI-VIRUS 8.5 FOR MICROSOFT ISA SERVER AND FOREFRONT TMG 10
CONFIGURATIONS MATERIELLES ET LOGICIELLES 11
ARCHITECTURE DE L'APPLICATION 13
Composition des modules et des sous-systèmes de Kaspersky Anti-Virus 13
Configuration de Kaspersky Anti-Virus 14
Scénarios d'analyse du trafic pris en charge 15
SCHEMAS TYPES DE DEPLOIEMENT DE L'APPLICATION 17
Serveur autonome 17
Groupe Autonome 18
Entreprise 20
DEPLOIEMENT DE L'APPLICATION 23
Préparation de l'installation 23
Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA Server / Forefront TMG 24
Installation d'applications complémentaires 24
Configuration des privilèges de l'utilisateur 24
Préparation du serveur SQL 25
Installation de l'application 25
Installation complète 26
Etape 1. Début de l'installation 27
Etape 2. Confirmation du Contrat de licence 27
Etape 3. Sélection du type d'installation 27
Etape 4. Sélection du dossier d'installation 27
Etape 5. Sélection du dossier de conservation des données 28
Etape 6. Configuration de la connexion à la base de données 29
Etape 7. Création de la règle pour l'administration à distance. 30
Etape 8. Lancement de la copie des fichiers et de l'enregistrement des modules 31
Etape 9. Copie des fichiers et enregistrement des modules 31
Etape 10. Fin de l'installation 31
Configuration initiale de l'application 31
Etape 1. Activation de l'application 32
Etape 2. Configuration des paramètres de mise à jour 32
Installation de la Console d'administration 33
Etape 1. Début de l'installation 33
Etape 2. Confirmation du Contrat de licence 33

Etape 3. Sélection du type d'installation 34
Etape 4. Sélection du dossier d'installation 34
Etape 5. Lancement de la copie des fichiers et de l'enregistrement des modules 35
Etape 6. Copie des fichiers et enregistrement des modules 35
Etape 7. Fin de l'installation 35
Connexion de la Console d'administration au stockage de configuration 35
Actions préalables avant la connexion de la Console d'administration 35
Connexion au stockage de configuration 36
Activation de l'application 38
Modifications dans le système après l'installation de l'application 39
Déplacement des serveurs Forefront TMG avec Kaspersky Anti-Virus 40
Ajout du serveur Forefront TMG EE au groupe autonome 41
Ajout du serveur Forefront TMG EE au groupe existant sous l'administration de EMS 41
Ajout du serveur Forefront TMG EE faisant partie du nouveau groupe à l'entreprise 42
Ajout du serveur Forefront TMG SE à l'entreprise 43
Exclusion du serveur du groupe ou de l'entreprise 44
Restauration de la configuration de Kaspersky Anti-Virus 44
Restauration de l'application 45
Suppression de l'application 45
A propos de la suppression de Kaspersky Anti-Virus 45
Suppression de l'application du serveur 47
CONTACTER LE SUPPORT TECHNIQUE 48
Modes d'obtention de l'assistance technique 48
Support Technique par téléphone 48
Obtention de l'assistance technique via Mon Espace Personnel 48
GLOSSAIRE 50
KASPERSKY LAB ZAO 53
INFORMATIONS SUR LE CODE TIERS 54
NOTIFICATIONS SUR LES MARQUES DE COMMERCE 55
INDEX 56

PRESENTATION DU MANUEL

Ce document représente le Manuel d'installation de Kaspersky Anti-Virus 8.5 for Microsoft® ISA Server and Forefront® TMG (ci-après - "Kaspersky Anti-Virus").

Ce manuel s'adresse aux experts techniques qui sont tenus d'installer et d'administrer Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG, ainsi que d'assister les entreprises qui utilisent Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG.

Il s'adresse aux experts techniques qui ont l'expérience de Microsoft ISA Server/Forefront TMG.

Le manuel est conçu pour les buts suivants :

- Donner une description des principes de fonctionnement de Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG, des exigences du système, des schémas typiques de déploiement, des particularités d'intégration avec d'autres applications.
- Aider à planifier le déploiement de Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG dans le réseau de l'entreprise.
- Décrire la préparation à l'installation de Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG, l'installation et l'activation de l'application.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

Dans ce document.....5

Conventions.....6

DANS CE DOCUMENT

Ce manuel contient les sections suivantes.

Sources d'informations sur l'application (à la page 8)

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

Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG (à la page 10)

Cette section décrit les possibilités générales de l'application.

Configurations matérielles et logicielles (à la page 11)

Cette section contient les informations sur les configurations matérielles et logicielles pour installer Kaspersky Anti-Virus.

Architecture de l'application (à la page 13)

Cette section contient la description des modules de Kaspersky Anti-Virus ou de la logique de leur interaction.

Schémas types de déploiement de l'application (à la page 17)

Cette section décrit les schémas types de déploiement de l'application au sein du réseau de l'entreprise ainsi que les particularités d'intégration avec les logiciels tiers.

Déploiement de l'application (à la page 23)

Cette section décrit les actions à exécuter avant l'installation de Kaspersky Anti-Virus et avant le début du fonctionnement de l'application, ainsi que les instructions d'installation, de restauration et de suppression de Kaspersky Anti-Virus.

Contacter le Support Technique (à la page 48)

Cette section contient des informations sur les moyens d'obtenir de l'assistance technique et sur les conditions requises pour obtenir l'aide du Support technique.

Glossaire (à la page 50)

Cette section contient une liste des termes utilisés dans l'application et une brève définition de chacun d'eux.

Kaspersky Lab (à la page 53)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (à la page 54)

Cette section contient des informations sur le code de programmation des éditeurs tiers utilisé dans l'application.

Notifications sur les marques de commerce (à la page 55)

Cette section répertorie les marques de commerce des titulaires de droit tiers utilisées dans ce document.

Index

Cette section permet de trouver rapidement les informations recherchées dans le document.

CONVENTIONS

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

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

Tableau 1. Conventions

EXEMPLE DU TEXTE	DESCRIPTION DES CONVENTIONS
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions indésirables potentielles qui peuvent amener à la perte d'informations, aux pannes de 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 ou des cas particuliers importants liés au fonctionnement de l'application.

EXEMPLE DU TEXTE	DESCRIPTION DES CONVENTIONS
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'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 mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
➧ *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
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 sur l'écran par l'application ; • données à saisir par l'utilisateur.
<Nom de l'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web 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 les recherches indépendantes 8

Discussion sur les logiciels de Kaspersky Lab sur le forum 9

Contacter le service commercial 9

Contacter le Groupe de localisation et de documentation 9

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

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

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

Si vous n'avez pas trouvé la solution au problème, nous vous recommandons de prendre contact avec le Support Technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 48).

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

Page sur le site Web de Kaspersky Lab

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

Cette page (http://www.kaspersky.com/fr/anti-virus-microsoft-isa-server-forefront-tmg) fournit des informations générales sur l'application, ses possibilités et ses particularités de fonctionnement.

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

Page sur le site Web du Support Technique (Base de connaissances)

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

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/tmg_8_ee) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Anti-Virus, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est offerte sous forme de l'aide contextuelle. L'aide contextuelle contient la liste et la description des paramètres pour chaque fenêtre de l'application.

Documentation

La distribution de l'application comprend les documents qui vous permettent d'installer et d'activer l'application sur les ordinateurs du réseau de l'entreprise, de configurer ses paramètres de fonctionnement et de connaître les principales astuces d'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB SUR LE FORUM

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

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

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service commercial à l'aide d'un des moyens suivants :

- En appelant notre service clientèle français (http://www.kaspersky.com/fr/contacts).
- En envoyant un message avec votre question à l'adresse sales@kaspersky.com.

La réponse sera donnée en français ou en anglais suivant votre demande.

CONTACTER LE GROUPE DE LOCALISATION ET DE DOCUMENTATION

Pour contacter le Groupe de localisation et de documentation, vous pouvez envoyer un message par courrier électronique à docfeedback@kaspersky.com. Vous devez indiquer "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.5 for Microsoft ISA Server et Forefront TMG" dans l'objet du message.

KASPERSKY ANTI-VIRUS 8.5 FOR MICROSOFT ISA SERVER AND FOREFRONT TMG

Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG assure une protection antivirus du trafic via les protocoles HTTP, FTP, SMTP et POP3 qui passe par le pare-feu de Microsoft ISA Server/Forefront TMG. Pour assurer la protection antivirus, les modules de Kaspersky Anti-Virus sont installés sur les serveurs physiques du réseau de l'entreprise sur lesquels est déployé le pare-feu de Microsoft ISA Server / Forefront TMG (ci-après "serveurs"). En fonction de l'option de déploiement du pare-feu de Microsoft ISA Server / Forefront TMG, les serveurs peuvent fonctionner de manière autonome ou être rassemblés dans un groupe ou une entreprise.

L'analyse du trafic via le protocole HTTPS est aussi prévue pour Kaspersky Anti-Virus installé sur Forefront TMG. Pour que l'analyse du trafic HTTPS soit exécutée, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

Kaspersky Anti-Virus offre les possibilités suivantes :

- L'analyse du trafic via les protocoles HTTP, FTP, SMTP, POP3 en temps réel à la recherche de la présence d'objets malveillants et d'objets potentiellement infectés. Selon les paramètres installés, Kaspersky Anti-Virus répare ou bloque ces objets.
- L'administration des stratégies de traitement des protocoles, de l'analyse antivirus, des exclusions de l'analyse pour différents groupes d'objets de réseau.
- La configuration des paramètres de productivité de l'application sur chaque serveur, en particulier, pour répartir la charge entre les processeurs du serveur.
- La configuration des paramètres généraux de fonctionnement de l'application pour tous les serveurs dans le groupe, tels que les paramètres de mise à jour, les paramètres de la sauvegarde et des journaux.
- La mise à jour programmée ou manuelle des bases de Kaspersky Anti-Virus. Les serveurs HTTP des mises à jour de Kaspersky Lab, les serveurs d'utilisateur HTTP, FTP ou le dossier réseau contenant l'ensemble réel des mises à jour peuvent servir de source de mise à jour.
- La configuration des paramètres de fonctionnement de l'application conformément au volume du trafic, en particulier, la configuration de la vitesse de transfert des données pour optimiser l'analyse.
- La conservation des copies des objets détectés par Kaspersky Anti-Virus dans la Sauvegarde.
- La conservation centralisée des informations sur les objets de la Sauvegarde dans la base de données.
- Administration des clés. La licence de Kaspersky Anti-Virus est octroyée pour toute l'application et non par pour des serveurs séparés.
- La surveillance en temps réel de l'application sur les serveurs.
- La consultation des statistiques générales d'utilisation de l'application sur les serveurs du groupe.
- L'administration des journaux des événements de l'application.
- La création des rapports de fonctionnement de l'application.

CONFIGURATIONS MATERIELLES ET LOGICIELLES

Kaspersky Anti-Virus peut fonctionner conjointement avec les produits suivants :

- Microsoft ISA Server 2006 avec SP1, Standard Edition (ci-après – Microsoft ISA Server SE).
- Microsoft ISA Server 2006, Enterprise Edition (ci-après – Microsoft ISA Server EE).
- Microsoft Forefront TMG 2010 avec SP1, Standard Edition (ci-après – Forefront TMG SE).
- Microsoft Forefront TMG 2010, Enterprise Edition (ci-après – Forefront TMG EE).

Exigences en cas d'utilisation de Kaspersky Anti-Virus sur le serveur Microsoft ISA Server SE/EE

Configuration matérielle :

- Processeur avec 1 GHz ;
- 1 Go de mémoire vive ;
- Espace disponible sur le disque dur : 2.5 Go.

Un des systèmes d'exploitation suivants est requis pour installer Kaspersky Anti-Virus :

- Microsoft Windows Server® 2003 32-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2003 R2 32-bits, Standard Edition/Enterprise Edition/Datacenter Edition.

Un des systèmes d'exploitation suivants est requis pour installer la Console d'administration de Kaspersky Anti-Virus :

- Microsoft Windows Server 2003 32-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2003 R2 32-bits, Standard Edition/Enterprise Edition/Datacenter Edition.
- Microsoft Windows® XP 32-bits avec SP3.

Exigences en cas d'installation de Kaspersky Anti-Virus sur le serveur Forefront TMG SE/EE

Configuration matérielle :

- Processeur 64-bits à 2 noyaux avec 2 GHz ;
- 2 Go de mémoire vive avec 1 GHz ;
- Espace disponible sur le disque dur : 2.5 Go.

Un des systèmes d'exploitation suivants est requis pour installer Kaspersky Anti-Virus :

- Microsoft Windows Server 2008 64-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2008 R2 64-bits, Standard Edition/Enterprise Edition/Datacenter Edition.

Un des systèmes d'exploitation suivants est requis pour installer la Console d'administration de Kaspersky Anti-Virus :

- Microsoft Windows Server 2008 R2 64-bits, Standard Edition/Enterprise Edition/Datacenter Edition.
- Microsoft Windows Server 2008 64-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows 7 64-bits, Professional Edition/Enterprise Edition/Ultimate Edition ;
- Microsoft Windows Vista® 64-bits avec SP2, Professional Edition/Business Edition/Enterprise Edition/Ultimate Edition.

Exigences vis-à-vis du serveur SQL sur lequel se trouve la Base de données de la sauvegarde et des statistiques

Un des systèmes d'administration des bases de données doit être installé sur le serveur :

- Microsoft SQL Server® 2008, Express Edition/Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2008 R2, Express Edition/Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2005, Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2005, Express Edition (+ Advanced Services).

ARCHITECTURE DE L'APPLICATION

Cette section contient la description des modules de Kaspersky Anti-Virus ou de la logique de leur interaction.

DANS CETTE SECTION

Composition des modules et des sous-systèmes de Kaspersky Anti-Virus.....13

Configuration de Kaspersky Anti-Virus 14

Scénarios d'analyse du trafic pris en charge 15

COMPOSITION DES MODULES ET DES SOUS-SYSTEMES DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus inclut les composants suivants :

- Le **Serveur de sécurité** est un composant assurant la fonctionnalité antivirus. Lors de l'installation, le module s'intègre au serveur Microsoft ISA Server/Forefront TMG.
- La **Console d'administration** est un module représentant l'outil Microsoft Management Console (ci-après - MMC). La console offre l'accès à l'administration de Kaspersky Anti-Virus et au contrôle de son fonctionnement.
- La **Base de données de la sauvegarde et des statistiques** est une base de données sur le serveur SQL conçue pour conserver les informations statistiques sur l'utilisation de l'application et les informations sur les objets dangereux dont les copies sont placées dans la sauvegarde par Kaspersky Anti-Virus.

Les modules Serveur de sécurité et Console d'administration s'installent sur le serveur où est déployé le pare-feu de Microsoft ISA Server/Forefront TMG. La Console d'administration peut être aussi installée sur un ordinateur séparé ayant accès au serveur où est installé le module Serveur de sécurité. En cas d'utilisation par plusieurs administrateurs, la Console d'administration peut être installée sur l'ordinateur de chaque administrateur.

La présence de la console Microsoft ISA Server/Forefront TMG, installée sur l'ordinateur, est une exigence indispensable pour installer la Console d'administration de Kaspersky Anti-Virus.

Le composant Serveur de sécurité inclut les sous-systèmes suivants :

- Les **Filtres de Kaspersky Anti-Virus** interceptent le trafic via les protocoles HTTP, FTP, SMTP et POP3, téléchargent les objets demandés par des postes clients et redirigent les objets téléchargés dans le sous-système d'analyse. Les filtres transmettent au poste client les objets demandés après l'analyse et délivrent la notification sur le blocage de l'objet.

  L'application inclut les filtres suivants :

  - Le filtre Web de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole HTTP.

    L'analyse du trafic via le protocole HTTPS est aussi prévue pour Kaspersky Anti-Virus installé sur Forefront TMG. Pour que l'analyse du trafic HTTPS soit exécutée, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

  - Le filtre FTP de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole FTP.

- Le filtre SMTP de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole SMTP.
- Le filtre POP3 de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole POP3.

Les filtres de Kaspersky Anti-Virus s'intègrent au pare-feu de Microsoft ISA Server/Forefront TMG lors de l'installation de l'application.

- Le **Sous-système d'analyse** est conçu pour l'analyse antivirus des objets. Le module d'analyse reçoit les objets téléchargés en provenance des filtres de Kaspersky Anti-Virus et les analyse à la recherche de la présence éventuelle de menaces. Le module utilise l'analyseur heuristique qui permet de détecter aussi les menaces inconnues. Après l'analyse, chaque objet se voit attribué un état qui détermine les actions suivantes à exécuter sur l'objet. Les objets sains sont ignorés sans modification, les autres sont traités conformément aux paramètres de l'analyse antivirus.
- Le **Sous-système de la mise à jour** assure la mise à jour des bases de Kaspersky Anti-Virus par leur téléchargement depuis les serveurs de mise à jour de Kaspersky Lab ou à partir d'autres sources indiquées.
- Le **Sous-système de la sauvegarde** assure la sauvegarde des copies de réserve des objets détectés par Kaspersky Anti-Virus durant l'analyse antivirus, ainsi que le transfert des informations sur les objets dans la Base de données de la sauvegarde et des statistiques. Ensuite, les objets de la Sauvegarde peuvent être supprimés ou enregistrés sur le disque local ou réseau. Les copies des objets sont enregistrées dans la Sauvegarde située sur le serveur où l'objet a été détecté. Les informations sur les objets placés dans la Sauvegarde sont enregistrées dans la Base de données de la sauvegarde et des statistiques.
- Le **Sous-système de configuration** assure la sauvegarde des paramètres de Kaspersky Anti-Virus.
- Le **Sous-système de licence** assure l'administration des clés et définit le statut de la licence de Kaspersky Anti-Virus. En cas de détection d'une violation du Contrat de licence, la fonctionnalité de Kaspersky Anti-Virus est limitée.
- Le **Sous-système de surveillance** assure la collecte des informations sur l'état de Kaspersky Anti-Virus.
- Le **Sous-système des statistiques** assure la collecte des statistiques sur les objets analysés. Les informations sont enregistrées dans la Base de données de la sauvegarde et des statistiques.
- Le **Sous-système de diagnostic** assure la gestion des journaux de fonctionnement de tous les modules de l'application. Les informations peuvent être enregistrées dans les fichiers texte, sauvegardées dans le journal des événements du système d'exploitation Microsoft Windows et transmises dans le sous-système des notifications Microsoft ISA Server/Forefront TMG
- Le **Sous-système des rapports** assure la réception des rapports sur les résultats du fonctionnement de Kaspersky Anti-Virus.

CONFIGURATION DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus peut fonctionner conjointement avec le pare-feu de Microsoft ISA Server/Forefront TMG dans les options de déploiement suivantes :

- Serveur autonome Microsoft ISA Server SE/EE ou Forefront TMG SE/EE.
- Groupe autonome des serveurs Forefront TMG EE sous l'administration du gestionnaire du groupe.
- Entreprise sur la base des serveurs Microsoft ISA Server EE ; un ou plusieurs groupes des serveurs Microsoft ISA EE sous l'administration de Configuration Storage Server (ci-après – CSS).
- Entreprise sur la base des serveurs Forefront TMG EE ; un ou plusieurs groupes des serveurs Forefront TMG EE sous l'administration de Enterprise Management Server (ci-après – EMS).
- Serveur Forefront TMG SE sous l'administration de EMS.

Les données de configuration de Kaspersky Anti-Virus s'enregistrent dans le stockage de configuration Microsoft ISA Server/Forefront TMG à l'installation de l'application. La configuration de Kaspersky Anti-Virus est partagée par niveaux logiques en conformité avec le partage par niveaux logiques de la configuration de Microsoft ISA Server/Forefront TMG.

En cas de déploiement de Kaspersky Anti-Virus dans l'entreprise, les paramètres de l'application sont répartis selon trois niveaux de configuration :

- niveau du serveur : paramètres applicables uniquement pour un serveur à part ;
- niveau de l'entreprise : paramètres applicables pour tous les serveurs du groupe sur lesquels Kaspersky Anti-Virus est installé.
- niveau de l'entreprise : paramètres applicables pour tous les serveurs de l'entreprise sur lesquels Kaspersky Anti-Virus est installé.

En cas de déploiement de Kaspersky Anti-Virus sur le serveur ou sur un groupe autonome, la configuration de l'application se compose de deux niveaux logiques : niveau du serveur et niveau du groupe.

La configuration du niveau du serveur se compose des paramètres de Kaspersky Anti-Virus qui dépendent des caractéristiques logicielles et matérielles du serveur sur lequel est installé le module Serveur de sécurité. Les autres paramètres de Kaspersky Anti-Virus concernent la configuration au niveau du groupe et de l'entreprise.

L'administration des paramètres de Kaspersky Anti-Virus est effectuée à l'aide de la Console d'administration qui se connecte au stockage de configuration de Microsoft ISA Server/Forefront TMG.

Les paramètres de Kaspersky Anti-Virus au niveau du serveur peuvent être configurés uniquement pour un serveur séparé parce qu'ils dépendent des caractéristiques matérielles et logicielles de l'ordinateur sur lequel l'application est installée. L'administration au niveau du groupe et/ou de l'entreprise est prévue pour d'autres paramètres de Kaspersky Anti-Virus. Les paramètres de Kaspersky Anti-Virus au niveau du groupe sont configurés de manière centralisée pour tous les serveurs inclus dans le groupe. Les paramètres de Kaspersky Anti-Virus du niveau de l'entreprise sont configurés de manière centralisée pour tous les serveurs de l'entreprise.

En cas de déploiement de l'application sur un serveur autonome, tous les paramètres sont configurés individuellement pour le serveur.

SCENARIOS D'ANALYSE DU TRAFIC PRIS EN CHARGE

Cette section décrit les particularités de fonctionnement de Kaspersky Anti-Virus dans les scénarios types suivants de trafic :

- Le client du réseau d'entreprise interne s'adresse aux ressources externes (outbound connection).
- Le client du réseau d'entreprise interne s'adresse aux ressources d'un autre réseau via le canal protégé (VPN) ;
- Le client en dehors du réseau d'entreprise s'adresse aux ressources situées dans le réseau d'entreprise interne et publiées par les outils Microsoft ISA Server/Forefront TMG (inbound connection) ;
- Le client en dehors du réseau d'entreprise, connecté via le canal protégé (VPN), s'adresse aux ressources internes du réseau d'entreprise.

Lorsque le client du réseau d'entreprise s'adresse aux ressources externes (outbound connection), l'analyse du trafic est exécutée de la manière suivante :

- Les objets téléchargés depuis les serveurs externes (download) sont analysés via les protocoles HTTP, HTTPS et FTP ; les objets téléchargés sur les serveurs externes ne sont pas analysés.

  Le trafic via le protocole HTTPS est analysé uniquement si Kaspersky Anti-Virus est installé sur le serveur Forefront TMG et si l'inspection du trafic HTTPS entrant est activée.

- Via les protocoles SMTP et POP3 : analyse de tous les messages transmis.

Lorsque le client du réseau d'entreprise s'adresse aux ressources d'un autre réseau via le canal protégé (VPN), l'analyse du trafic est exécutée de la même manière que lorsque le client du réseau d'entreprise s'adresse aux ressources externes.

Lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise publiées (inbound connection), l'analyse du trafic est exécutée de la manière suivante :

- Via les protocoles HTTP, HTTPS et FTP : le trafic des ressources d'entreprise au client est analysé ; le trafic du client aux ressources d'entreprise n'est pas analysé.

  Le trafic via le protocole HTTPS est analysé uniquement si Kaspersky Anti-Virus est installé sur le serveur Forefront TMG et si l'inspection du trafic HTTPS sortant est activée.

- Via les protocoles SMTP et POP3 : analyse de tous les messages transmis.

Lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise via le canal protégé (VPN), l'analyse du trafic est exécutée de la même manière que lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise publiées (inbound connection).

L'analyse des protocoles de chaque type est configurée dans les paramètres de Kaspersky Anti-Virus et peut être désactivée.

SCHEMAS TYPES DE DEPLOIEMENT DE L'APPLICATION

Cette section décrit les schémas types de déploiement de l'application au sein du réseau de l'entreprise ainsi que les particularités d'intégration avec les logiciels tiers.

Les schémas suivants de déploiement sont prévus pour Kaspersky Anti-Virus :

- *Serveur autonome* : Kaspersky Anti-Virus s'installe sur le serveur autonome Microsoft ISA Server / Forefront TMG SE ou EE (cf. section "Serveur autonome" à la page 17).
- *Groupe autonome* : Kaspersky Anti-Virus s'installe sur les serveurs qui font partie du groupe autonome des serveurs Forefront TMG (cf. section "Groupe autonome" à la page 18).
- *Entreprise* : Kaspersky Anti-Virus s'installe sur les serveurs Microsoft ISA/Forefront TMG qui font partie des groupes inclus dans l'entreprise sous l'administration de CSS ou EMS (cf. section "Entreprise" à la page 20).

Quel que soit le schéma de déploiement de Kaspersky Anti-Virus, l'installation de l'application est exécutée sur chaque serveur à part.

En cas de déploiement de Kaspersky Anti-Virus dans un groupe de serveurs, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

DANS CETTE SECTION

Serveur autonome 17

Groupe autonome 18

Entreprise 20

SERVEUR AUTONOME

Le schéma de déploiement *Serveur autonome* suppose l'installation de Kaspersky Anti-Virus sur le serveur autonome Microsoft ISA/Forefront TMG SE ou EE.

Les paramètres de Kaspersky Anti-Virus se trouvent dans le stockage de configuration de Microsoft ISA/Forefront TMG situé sur le serveur.

La configuration de Kaspersky Anti-Virus inclut les paramètres au niveau du serveur et du groupe (cf. section "Configuration de Kaspersky Anti-Virus" à la page 14). Tous les paramètres sont configurés individuellement pour le serveur.

Le schéma de déploiement *Serveur autonome* inclut les étapes suivantes :

1. Préparation de l'installation. Avant l'installation de Kaspersky Anti-Virus, procédez comme suit :
   - Supprimez du serveur sur lequel l'application est installée les versions antérieures de Kaspersky Anti-Virus et les autres applications antivirus pour Microsoft ISA Server / Forefront TMG (cf. section "Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA Server / Forefront TMG" à la page 24).
   - Installez sur le serveur les applications complémentaires nécessaires au fonctionnement des modules de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).

- Configurez les privilèges de l'utilisateur effectuant l'installation (cf. section "Configuration des privilèges de l'utilisateur" à la page 24).

- Préparez le serveur SQL sur lequel sera déployée la Base de données de la sauvegarde et des statistiques de Kaspersky Anti-Virus (cf. section "Préparation du serveur SQL" à la page 25).

2. Installation de Kaspersky Anti-Virus. L'installation complète de l'application est exécutée sur le serveur : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   La connexion à la Base de données de la sauvegarde et des statistiques est effectuée à l'une des étapes de l'Assistant d'installation. Vous devez indiquer le serveur correspondant à l'emplacement de la Base de données de la sauvegarde et des statistiques et les paramètres de connexion à cette dernière. Si la Base de données de la sauvegarde et des statistiques n'a pas été créée à l'étape de préparation à l'installation (cf. section "Préparation du serveur SQL" à la page 25), vous devez indiquer les paramètres de création de la base de données.

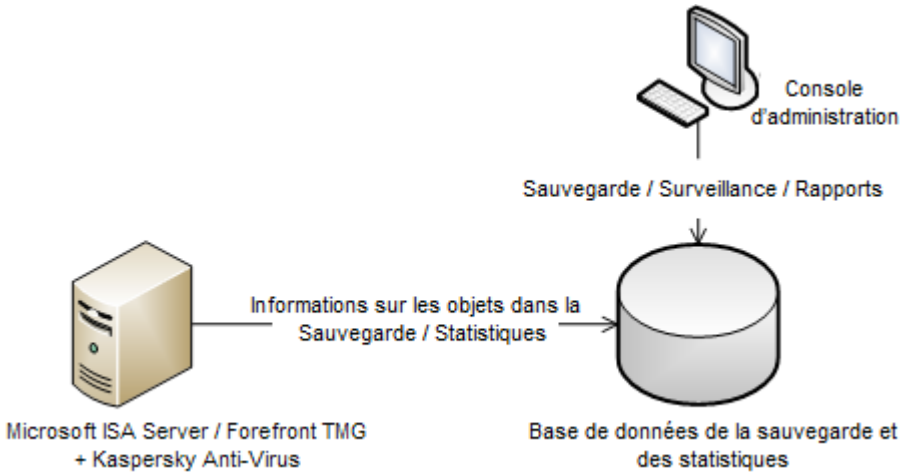

Illustration 1. Schéma de déploiement Serveur autonome

3. L'installation de la console d'administration complémentaire (cf. ill. ci-dessus). S'il est nécessaire d'administrer Kaspersky Anti-Virus à distance, vous devez installer sur un ordinateur séparé le module Console d'administration (cf. section "Installation de la Console d'administration" à la page 33).

4. Préparation de l'utilisation. Avant de commencer à utiliser Kaspersky Anti-Virus, il faut activer l'application (cf. section "Activation de l'application" à la page 38), si elle n'a pas été activée juste après l'installation (cf. section "Configuration initiale de l'application" à la page 31).

GROUPE AUTONOME

Le schéma de déploiement *Groupe autonome* suppose l'installation de Kaspersky Anti-Virus sur les serveurs qui font partie du groupe autonome de serveurs Forefront TMG.

Pour assurer une protection antivirus complète, il faut installer Kaspersky Anti-Virus sur chaque serveur du groupe.

Les paramètres de Kaspersky Anti-Virus se trouvent dans le stockage de configuration Forefront TMG situé sur un des serveurs du groupe (gestionnaire du groupe).

La configuration de Kaspersky Anti-Virus inclut les paramètres au niveau du serveur et du groupe (cf. section "Configuration de Kaspersky Anti-Virus" à la page 14). Les paramètres au niveau du groupe sont configurés de manière centralisée pour tous les serveurs du groupe.

Tous les serveurs du groupe se connectent à une Base de données de la sauvegarde et des statistiques.

Le schéma de déploiement *Matrice autonome* inclut les étapes suivantes :

1. Préparation de l'installation. Avant l'installation de Kaspersky Anti-Virus, procédez comme suit :

   - Depuis chaque serveur sur lequel est installée l'application, supprimez les versions antérieures de Kaspersky Anti-Virus les autres applications antivirus pour Microsoft ISA Server / Forefront TMG (cf. section "Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA/Forefront TMG" à la page 24).

   - Installez sur les serveurs les applications complémentaires nécessaires au fonctionnement de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).

   - Configurez les privilèges de l'utilisateur effectuant l'installation (cf. section "Configuration des privilèges de l'utilisateur" à la page 24).

   - Préparez le serveur SQL sur lequel sera déployée la Base de données de la sauvegarde et des statistiques de Kaspersky Anti-Virus (cf. section "Préparation du serveur SQL" à la page 25).

2. Installation de Kaspersky Anti-Virus sur le premier serveur du groupe. L'installation complète de l'application est exécutée sur le serveur : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   La connexion à la Base de données de la sauvegarde et des statistiques est effectuée à l'une des étapes de l'Assistant d'installation. Vous devez indiquer le serveur correspondant à l'emplacement de la Base de données de la sauvegarde et des statistiques et les paramètres de connexion à cette dernière. Si la Base de données de la sauvegarde et des statistiques n'a pas été créée à l'étape de préparation à l'installation (cf. section "Préparation du serveur SQL" à la page 25), vous devez indiquer les paramètres de création de la base de données.

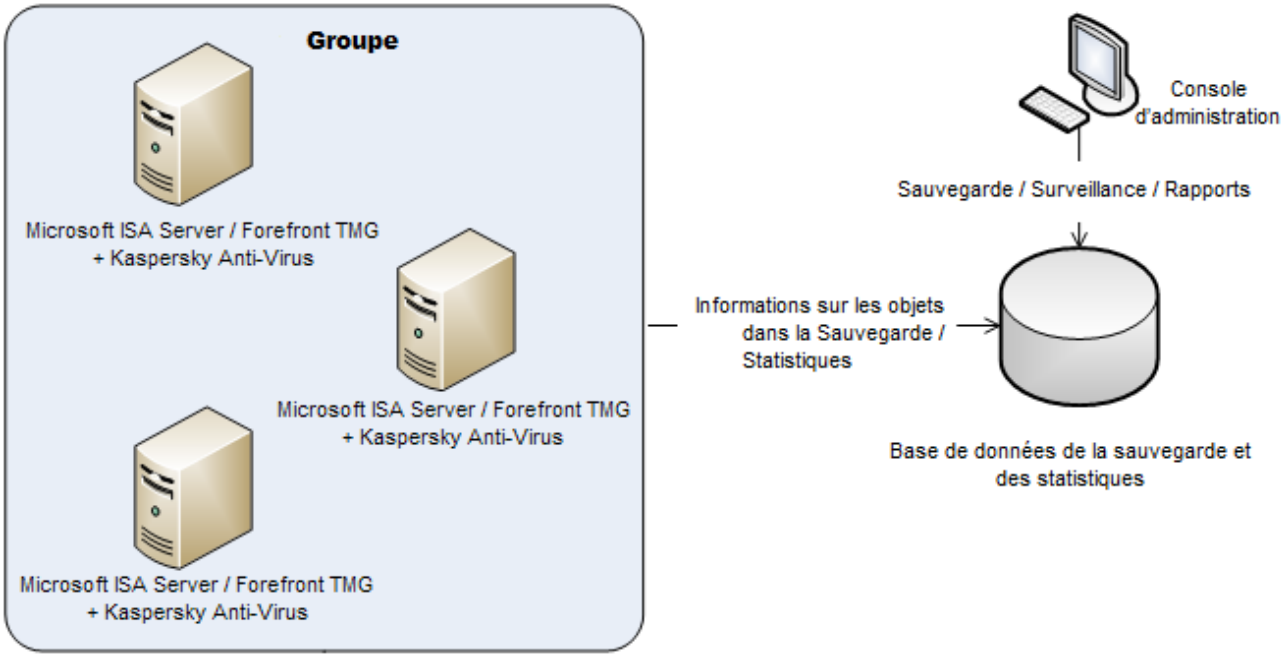

Illustration 2. Schéma de déploiement Groupe Autonome

3. Installation de Kaspersky Anti-Virus sur le deuxième serveur et les serveurs suivants du groupe. L'installation complète de l'application est exécutée successivement sur chaque serveur du groupe. Les modules Serveur de sécurité et Console d'administration sont installés sur les serveurs (cf. section "Installation complète" à la page 26).

   Tous les serveurs se connectent automatiquement à la Base de données de la sauvegarde et des statistiques indiquée lors de l'installation de Kaspersky Anti-Virus sur le premier serveur du groupe.

4. L'installation de la console d'administration complémentaire (cf. ill. ci-dessus). S'il est nécessaire d'administrer Kaspersky Anti-Virus à distance, vous devez installer sur un ordinateur séparé le module Console d'administration (cf. section "Installation de la Console d'administration" à la page 33).

5. Préparation de l'utilisation. Avant de commencer à utiliser Kaspersky Anti-Virus, il faut activer l'application (cf. section "Activation de l'application" à la page 38), si elle n'a pas été activée juste après l'installation (cf. section "Configuration initiale de l'application" à la page 31).

ENTREPRISE

Le schéma de déploiement *Entreprise* suppose l'installation de Kaspersky Anti-Virus sur les serveurs Microsoft ISA Server qui font partie des groupes inclus dans l'entreprise sous l'administration de CSS, ou sur les serveurs Forefront TMG qui font partie des groupes inclus dans l'entreprise sous l'administration de EMS.

L'option d'installation de Kaspersky Anti-Virus sur les serveurs Forefront TMG SE sous l'administration de EMS est un cas fréquent pour le schéma de déploiement *Entreprise*. Le serveur Forefront TMG SE se joint à l'entreprise faisant partie du groupe contenant uniquement ce serveur.

Kaspersky Anti-Virus peut être installé sur un ou plusieurs groupes faisant partie de l'entreprise.

En cas de déploiement de Kaspersky Anti-Virus dans un groupe de serveurs, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

Les paramètres de Kaspersky Anti-Virus se trouvent dans le stockage de configuration de Microsoft ISA/Forefront TMG situé dans CSS pour Microsoft ISA Server ou dans EMS pour Forefront TMG.

La configuration de Kaspersky Anti-Virus inclut les paramètres au niveau du serveur, du groupe et de l'entreprise (cf. section "Configuration de Kaspersky Anti-Virus" à la page 14). Les paramètres au niveau du groupe sont configurés de manière centralisée pour tous les serveurs d'un seul groupe. Les paramètres au niveau de l'entreprise sont communs pour tous les serveurs de l'entreprise sur lesquels Kaspersky Anti-Virus est installé et sont configurés au niveau de l'entreprise.

En cas d'installation de Kaspersky Anti-Virus sur plusieurs groupes de serveurs faisant partie de l'entreprise, il est possible d'utiliser une Base de données de la sauvegarde et des statistiques unique pour tous les groupes de l'entreprise, ou des bases particulières de données pour chaque groupe ou ensemble de groupes.

Les statistiques centralisées (dans le cadre de l'entreprise) et la sauvegarde centralisée des informations sur les objets placés dans la Sauvegarde sont prises en charge uniquement si tous les serveurs de l'entreprise utilisent une Base de données de la sauvegarde et des statistiques unique.

Le schéma de déploiement *Entreprise* inclut les étapes suivantes :

1. Préparation de l'installation. Avant l'installation de Kaspersky Anti-Virus, procédez comme suit :

   - Depuis chaque serveur sur lequel est installée l'application, supprimez les versions antérieures de Kaspersky Anti-Virus les autres applications antivirus pour Microsoft ISA Server / Forefront TMG (cf. section "Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA/Forefront TMG" à la page 24).

   - Installez sur les serveurs les applications complémentaires nécessaires au fonctionnement de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).

   - Configurez les privilèges de l'utilisateur effectuant l'installation (cf. section "Configuration des privilèges de l'utilisateur" à la page 24).

   - Préparez le serveur SQL sur lequel sera déployée la Base de données de la sauvegarde et des statistiques de Kaspersky Anti-Virus (cf. section "Préparation du serveur SQL" à la page 25).

2. Installation de Kaspersky Anti-Virus sur le premier serveur du premier groupe. L'installation complète de l'application est exécutée sur le serveur : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   La connexion à la Base de données de la sauvegarde et des statistiques est effectuée à l'une des étapes de l'Assistant d'installation. Vous devez indiquer le serveur correspondant à l'emplacement de la Base de données de la sauvegarde et des statistiques et les paramètres de connexion à cette dernière. Si la Base de données de la sauvegarde et des statistiques n'a pas été créée à l'étape de préparation à l'installation (cf. section "Préparation du serveur SQL" à la page 25), vous devez indiquer les paramètres de création de la base de données.

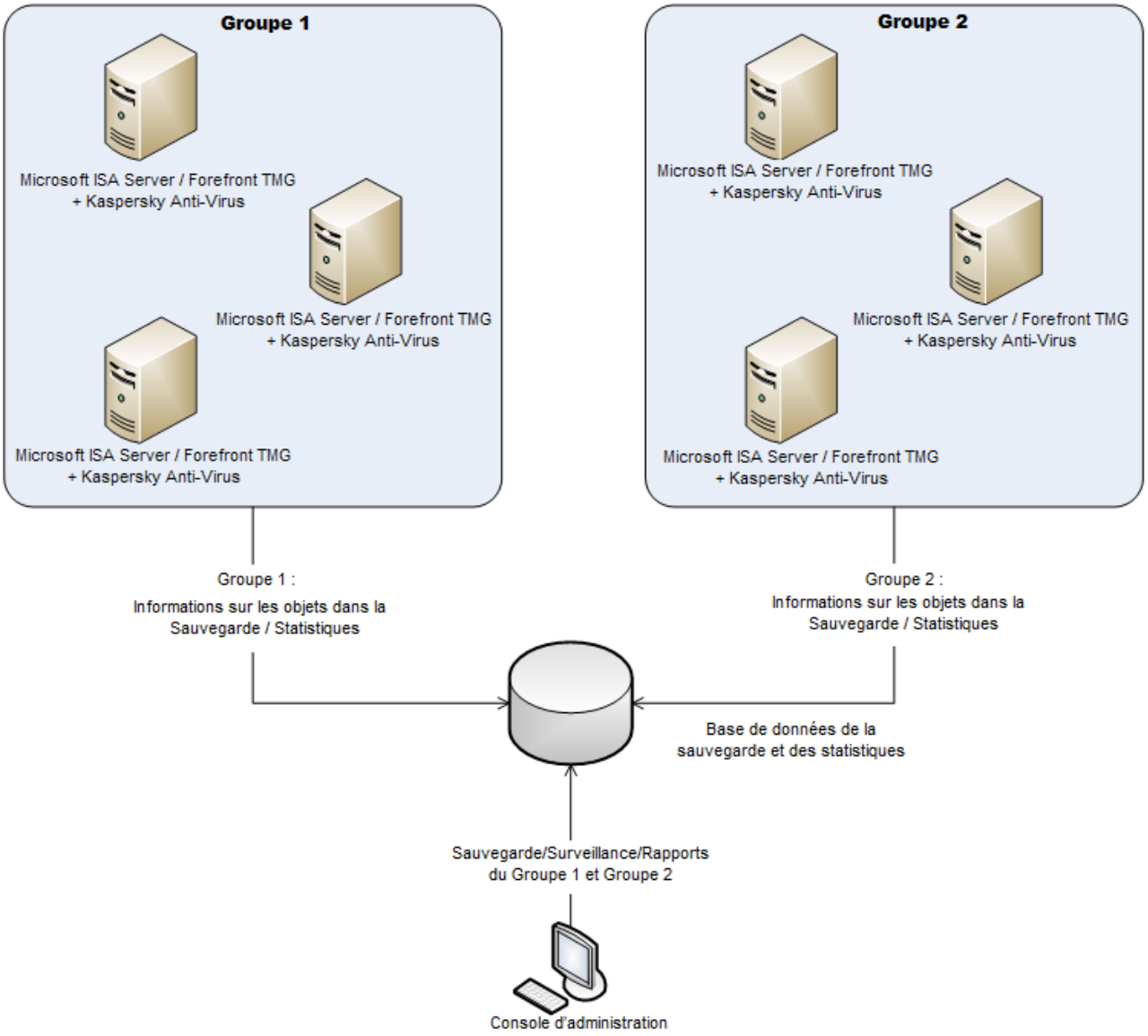

Illustration 3. Schéma de déploiement Entreprise : Base de données de la sauvegarde et des statistiques unique

3. Installation de Kaspersky Anti-Virus sur le deuxième serveur et les serveurs suivants du premier groupe. L'installation complète de l'application est exécutée sur chaque serveur du groupe : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   Tous les serveurs du premier groupe se connectent automatiquement à la Base de données de la sauvegarde et des statistiques indiquée lors de l'installation de Kaspersky Anti-Virus sur le premier serveur du groupe.

4. Installation de Kaspersky Anti-Virus sur le premier serveur du deuxième groupe. L'installation complète de l'application est exécutée sur le serveur : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   Une des étapes de l'Assistant d'installation permet de sélectionner la Base de données de la sauvegarde et des statistiques pour les serveurs du deuxième groupe : il est possible d'utiliser la même Base de données de la sauvegarde et des statistiques à laquelle tous les serveurs du premier groupe ont été connectés, ou d'indiquer le serveur d'emplacement et les paramètres de création de la nouvelle Base de données de la sauvegarde et des statistiques ou de connexion à une autre Base de données de la sauvegarde et des statistiques (cf. ill. ci-après)

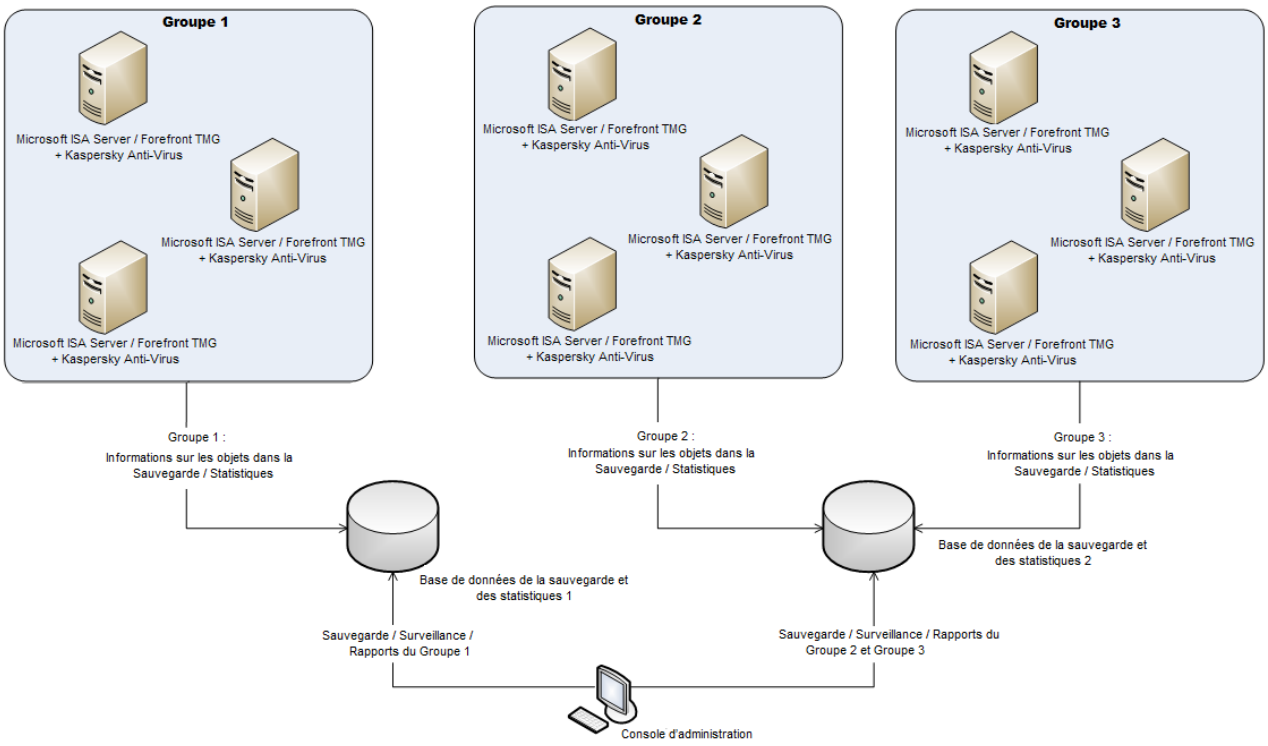

Illustration 4. Schéma de déploiement Entreprise : plusieurs bases de données de la sauvegarde et des statistiques

5. Installation de Kaspersky Anti-Virus sur le deuxième serveur et les serveurs suivants du deuxième groupe. L'installation complète de l'application est exécutée sur chaque serveur du groupe : installation des modules Serveur de sécurité et Console d'administration (cf. section "Installation complète" à la page 26).

   Tous les serveurs du deuxième groupe se connectent automatiquement à la Base de données de la sauvegarde et des statistiques indiquée lors de l'installation de Kaspersky Anti-Virus sur le premier serveur du deuxième groupe.

   L'installation de Kaspersky Anti-Virus sur les serveurs du troisième groupe et des groupes suivants de l'entreprise est exécutée de la même manière que sur les serveurs du deuxième groupe (cf. étapes 4 et 5).

6. L'installation de la console d'administration complémentaire (cf. ill. ci-dessus). S'il est nécessaire d'administrer Kaspersky Anti-Virus à distance, vous devez installer sur un ordinateur séparé le module Console d'administration (cf. section "Installation de la Console d'administration" à la page 33).

7. Préparation de l'utilisation. Avant de commencer à utiliser Kaspersky Anti-Virus, il faut activer l'application (cf. section "Activation de l'application" à la page 38), si elle n'a pas été activée juste après l'installation (cf. section "Configuration initiale de l'application" à la page 31).

DEPLOIEMENT DE L'APPLICATION

Cette section contient les informations suivantes :

- la description des actions à exécuter avant d'installer Kaspersky Anti-Virus et avant d'utiliser l'application ;
- les instructions d'installation et de suppression de Kaspersky Anti-Virus ;
- les modifications s'opérant dans le système suite à l'installation de l'application ;
- la description de la procédure de restauration de Kaspersky Anti-Virus ;
- la description des conséquences du déplacement des serveurs Forefront TMG EE / SE sur lesquels est installé Kaspersky Anti-Virus et les recommandations de restauration de l'application en cas de violation de la configuration.

DANS CETTE SECTION

Préparation de l'installation. 23

Installation de l'application 25

Connexion de la Console d'administration au stockage de configuration 35

Activation de l'application 38

Modifications dans le système après l'installation de l'application 39

Déplacement des serveurs Forefront TMG avec Kaspersky Anti-Virus installé 40

Restauration de l'application 45

Suppression de l'application 45

PREPARATION DE L'INSTALLATION

Avant l'installation de Kaspersky Anti-Virus, procédez comme suit :

- Supprimer du serveur sur lequel est installée l'application les versions antérieures de Kaspersky Anti-Virus les autres applications antivirus pour Microsoft ISA Server / Forefront TMG (cf. section "Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA/Forefront TMG" à la page 24).
- Installer sur le serveur sur lequel est installée l'application, les applications complémentaires nécessaires au fonctionnement de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).
- Configurer les privilèges de l'utilisateur effectuant l'installation (cf. section "Configuration des privilèges de l'utilisateur" à la page 24).
- Préparer le serveur SQL sur lequel sera déployée la Base de données de la sauvegarde et des statistiques de Kaspersky Anti-Virus (cf. section "Préparation du serveur SQL" à la page 25).

Avant de commencer l'installation, il faut s'assurer que les configurations matérielles et logicielles de l'ordinateur correspondent aux exigences de Kaspersky Anti-Virus (cf. section "Configurations matérielle et logicielle" à la page 11).

DANS CETTE SECTION

Suppression des versions antérieures de Kaspersky Anti-Virus et des autres applications antivirus pour Microsoft ISA Server / Forefront TMG....24

Installation d'applications complémentaires....24

Configuration des privilèges de l'utilisateur....24

Préparation du serveur SQL....25

SUPPRESSION DES VERSIONS ANTERIEURES DE KASPERSKY ANTI-VIRUS ET DES AUTRES APPLICATIONS ANTIVIRUS POUR MICROSOFT ISA SERVER / FOREFRONT TMG

L'utilisation simultanée de Kaspersky Anti-Virus avec d'autres applications antivirus pour Microsoft ISA Server / Forefront TMG peut entraîner un dysfonctionnement de Kaspersky Anti-Virus.

Si d'autres applications antivirus pour Microsoft ISA Server / Forefront TMG ou d'autres versions de Kaspersky Anti-Virus pour Microsoft ISA Server / Forefront TMG sont installées sur l'ordinateur, il est recommandé de les supprimer avant d'installer Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG.

INSTALLATION D'APPLICATIONS COMPLEMENTAIRES

Avant de commencer à installer les modules de Kaspersky Anti-Virus, vous devez installer sur l'ordinateur les applications complémentaires suivantes :

- Microsoft Windows Installer 3.1.
- Microsoft Management Console 3.0.
- Microsoft .NET Framework 3.5 SP1.

CONFIGURATION DES PRIVILEGES DE L'UTILISATEUR

Le compte utilisateur qui effectue l'installation doit posséder les privilèges d'un des rôles administratifs de Microsoft ISA Server / Forefront TMG.

- *Administrateur du groupe Microsoft ISA Server/Forefront TMG*. L'utilisateur doté du rôle *Administrateur du groupe ISA Server/Forefront TMG* possède les privilèges d'installation de Kaspersky Anti-Virus sur les serveurs du groupe dont il est l'administrateur.
- *Administrateur de l'entreprise Microsoft ISA Server/Forefront TMG*. L'utilisateur doté du rôle *Administrateur de l'entreprise ISA Server / Forefront TMG* possède les privilèges d'installation de Kaspersky Anti-Virus sur tous les serveurs de l'entreprise.

Avant de commencer l'installation, assurez-vous que votre compte possède les privilèges indiqués.

L'installation de l'application n'est pas autorisée si l'utilisateur effectuant l'installation possède les privilèges d'un des rôles suivants :

- *Auditeur de l'entreprise Microsoft ISA Server/Forefront TMG* ;
- *Auditeur du groupe Microsoft ISA Server/Forefront TMG* ;
- *Auditeur d'observation du groupe Microsoft ISA Server / Forefront TMG*.

En cas de tentative d'installation de l'application sous un compte utilisateur qui possède l'un de ces rôles, l'Assistant d'installation affiche un message indiquant que les privilèges d'installation sont insuffisants.

PREPARATION DU SERVEUR SQL

Au cours de l'installation de Kaspersky Anti-Virus, vous devez indiquer les paramètres de connexion du module Serveur de sécurité à la base de données sur laquelle seront conservées les informations relatives aux objets de la sauvegarde et des statistiques du serveur où est installé le module Serveur de sécurité (c'est-à-dire à la *Base de données de la sauvegarde et des statistiques*). La Base de données de la sauvegarde et des statistiques peut être créée sur le serveur SQL avant ou pendant l'installation de Kaspersky Anti-Virus.

Pour préparer le serveur SQL, procédez comme suit :

1. Assurez-vous que le serveur sur lequel est installé le système d'administration de la base de données de Microsoft SQL Server peut échanger les données avec le serveur à partir duquel il conservera les informations.
2. Exécutez une des actions suivantes :
   - Si vous souhaitez préparer la base de données à l'avance, créez sur le serveur SQL une base de données et configurez un compte qui possède les privilèges de lecture et d'enregistrement des informations dans la base de données.
   - Si vous souhaitez que l'Assistant d'installation crée une base de données pendant l'installation de Kaspersky Anti-Virus, configurez un compte utilisateur qui possède les privilèges de création d'une base de données, de déploiement d'un schéma de base de données ainsi que de lecture et d'enregistrement des informations dans la base de données.

   Le compte, indiqué lors de l'installation, sert à utiliser la Base de données de la sauvegarde et des statistiques. En cas de besoin, vous pouvez modifier les paramètres de connexion à la Base de données de la sauvegarde et des statistiques après l'installation de Kaspersky Anti-Virus dans la Console d'administration de l'application (pour de plus amples informations, cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

INSTALLATION DE L'APPLICATION

Cette section décrit l'installation de Kaspersky Anti-Virus sur le serveur.

Peu importe le schéma de déploiement de Kaspersky Anti-Virus, l'installation de Kaspersky Anti-Virus est exécutée sur chaque serveur à part.

En cas de déploiement de Kaspersky Anti-Virus dans un groupe de serveurs, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

Il existe les types d'installation suivants :

- *Installation complète* : Installation des modules Serveur de sécurité et Console d'administration sur l'ordinateur (cf. section "Installation complète" à la page 26). Microsoft ISA Server / Forefront TMG doit être installé sur l'ordinateur (cf. section "Configurations matérielles et logicielles" à la page 11).

- *Installation de la Console d'administration* : seule la Console d'administration de Kaspersky Anti-Virus est installée sur l'ordinateur (cf. section "Installation de la Console d'administration" à la page 33). La Console d'administration de Microsoft ISA Server/Forefront TMG doit être installée sur l'ordinateur.

Il est impossible d'installer le module Serveur de sécurité de Kaspersky Anti-Virus sans la Console d'administration.

Toutes les opérations d'installation de l'application sont exécutées dans les fenêtres de l'Assistant d'installation. Vous pouvez gérer le processus d'installation à l'aide des boutons situés dans la partie inférieure de la fenêtre de l'Assistant. Pour passer à l'étape suivante d'installation, cliquez sur le bouton **Suivant**. Pour retourner à l'étape précédente d'installation, cliquez sur le bouton **Précédent**.

Vous pouvez refuser d'installer l'application à n'importe quelle étape de l'Assistant d'installation. Pour annuler l'installation de Kaspersky Anti-Virus, cliquez sur le bouton **Annuler**. Avant de terminer, l'Assistant d'installation supprime toutes les modifications qu'il a apportées au système.

Si une erreur survient pendant l'installation, l'Assistant d'installation affiche un message d'erreur. Si l'Assistant d'installation ne peut pas poursuivre l'installation de l'application pour une raison quelconque, il supprime toutes les modifications apportées au système. Pour fermer la fenêtre de l'Assistant d'installation, cliquez sur le bouton **Terminer**.

DANS CETTE SECTION

Installation complète 26

Configuration initiale de l'application 31

Installation de la Console d'administration 33

INSTALLATION COMPLETE

Cette section décrit l'installation complète de Kaspersky Anti-Virus sur le serveur à l'aide de l'Assistant d'installation :

DANS CETTE SECTION

Etape 1. Début de l'installation 27

Etape 2. Confirmation du Contrat de licence 27

Etape 3. Sélection du type d'installation 27

Etape 4. Sélection du dossier d'installation 27

Etape 5. Sélection du dossier de conservation des données 28

Etape 6. Configuration de la connexion à la base de données 29

Etape 7. Création de la règle pour l'administration à distance. 30

Etape 8. Lancement de la copie des fichiers et de l'enregistrement des modules 31

Etape 9. Copie des fichiers et enregistrement des modules 31

Etape 10. Fin de l'installation 31

ETAPE 1. DEBUT DE L'INSTALLATION

Pour commencer l'installation de Kaspersky Anti-Virus, lancez sur le serveur le fichier exécutable kav4isa_8.5.XXXX_ee_ru.exe (où XXXX correspond au numéro de version) qui fait partie de la distribution.

La fenêtre de l'Assistant d'installation s'ouvre.

Si l'Assistant d'installation a détecté sur le serveur une version antérieure de Kaspersky Anti-Virus for Microsoft ISA Server / Forefront TMG, l'écran affiche une notification et l'Assistant d'installation se termine.

L'Assistant d'installation vérifie la présence sur le serveur d'applications complémentaires nécessaires au fonctionnement de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).

Si des applications complémentaires nécessaires manquent, l'écran affiche un avertissement et l'Assistant d'installation se termine. Installez les applications complémentaires nécessaires et relancez l'Assistant d'installation de Kaspersky Anti-Virus.

ETAPE 2. CONFIRMATION DU CONTRAT DE LICENCE

Lisez le Contrat de licence. Pour poursuivre l'installation, vous devez accepter les conditions du contrat.

Pour accepter les conditions du Contrat de licence, cochez la case **J'accepte les conditions du Contrat de licence**.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Cliquez sur le bouton **Complète** pour installer sur le serveur les modules Serveur de sécurité et Console d'administration.

Le bouton **Complète** est inaccessible si la configuration matérielle et logicielle de l'ordinateur ne correspond pas aux exigences de Kaspersky Anti-Virus (cf. section "Configurations matérielles et logicielles" à la page 11).

Pour installer les modules de Kaspersky Anti-Virus, l'espace disponible sur le disque dur doit être de 2,5 Go.

Le module Console d'administration peut être également installé sur un ordinateur séparé pour administrer à distance Kaspersky Anti-Virus (cf. section "Installation de la Console d'administration" à la page 33).

ETAPE 4. SELECTION DU DOSSIER D'INSTALLATION

Si vous effectuez l'installation sur un serveur autonome ou sur le premier serveur du groupe, vous devez indiquer le dossier dans lequel seront installés les modules de Kaspersky Anti-Virus.

Si vous installez Kaspersky Anti-Virus sur le deuxième serveur ou les serveurs suivants du groupe, l'Assistant d'installation affiche le chemin d'accès au dossier d'installation sélectionné lors de l'installation de l'application sur le premier serveur du groupe. Avec cela, vous ne pouvez pas modifier le chemin d'accès au dossier d'installation.

Kaspersky Anti-Virus doit être installé sur le même disque où est installé Microsoft ISA Server / Forefront TMG. Si le disque dur sélectionné pour installer l'application sur le premier serveur du groupe est absent sur le deuxième serveur ou les serveurs suivants du groupe, l'Assistant d'installation affiche le chemin d'accès au dossier d'installation par défaut.

Pour indiquer le dossier dans lequel seront installés les modules de Kaspersky Anti-Virus, cliquez sur le bouton **Parcourir** (cf. ill. ci-dessous). Dans la fenêtre qui s'ouvre, sélectionnez le dossier ou saisissez le chemin du dossier manuellement.

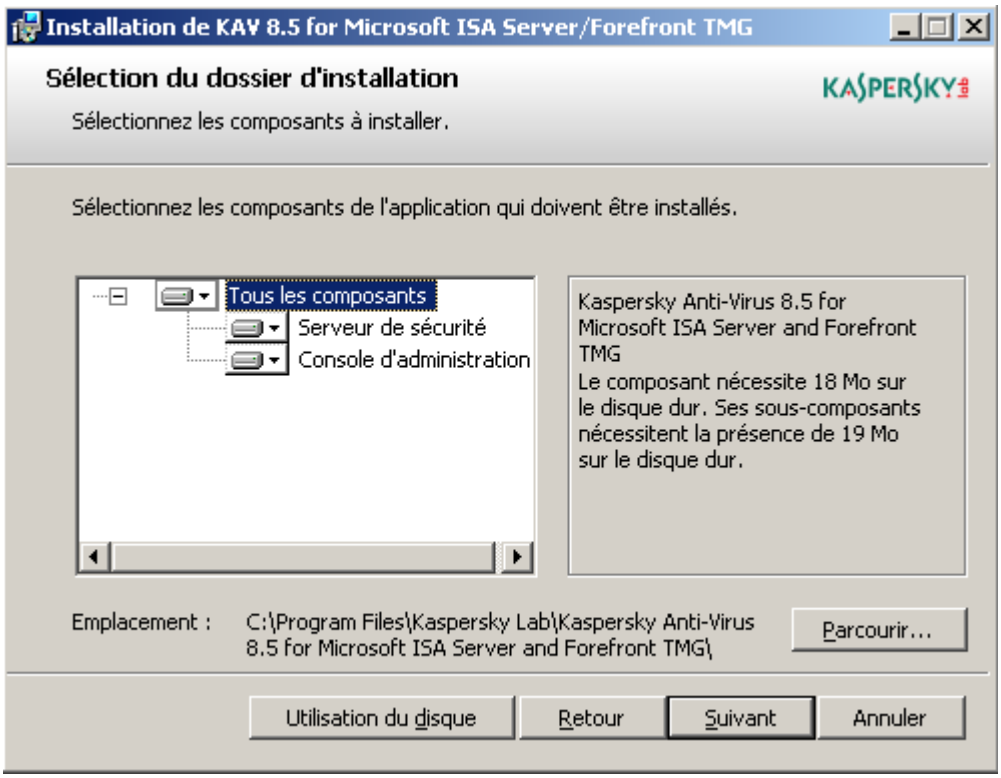

Illustration 5. Sélection du dossier d'installation : installation complète

Si vous avez indiqué un dossier inexistant, l'Assistant créera le dossier avec le nom indiqué.

Par défaut, Kaspersky Anti-Virus est installé dans le dossier <ProgramFiles>\Kaspersky Lab\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG, où <ProgramFiles> peut avoir l'une des valeurs suivantes :

- %ProgramFiles% (sous un système d'exploitation 32-bits) ou %ProgramFiles(x86)% (sous un système d'exploitation 64-bits) : si Microsoft ISA Server / Forefront TMG est installé sur le même disque que le système d'exploitation Microsoft Windows;
- <Disque avec Microsoft ISA Server / Forefront TMG>:\Program Files : si Microsoft ISA Server / Forefront TMG et le système d'exploitation Microsoft Windows sont installés sur des disques différents.

ETAPE 5. SELECTION DU DOSSIER DE CONSERVATION DES DONNEES

Vous devez indiquer le dossier sur le disque dur sur lequel seront installées les données créées pendant le fonctionnement de Kaspersky Anti-Virus.

Pour indiquer le dossier de sauvegarde de l'application, cliquez sur le bouton **Modifier**. Dans la fenêtre qui s'ouvre, sélectionnez le dossier ou saisissez le chemin du dossier manuellement.

Si vous avez indiqué un dossier inexistant, l'Assistant créera le dossier avec le nom indiqué.

Par défaut, pour conserver les données créées pendant le fonctionnement de l'application, le dossier <CommonAppDataFolder>\Kaspersky Lab\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG\data est utilisé, où <CommonAppDataFolder> peut avoir l'une des valeurs suivantes :

- %AllUsersProfile%\Application Data : pour Microsoft Windows XP et Microsoft Windows Server 2003 ;
- %ProgramData% : pour Microsoft Windows Server 2008 et Microsoft Windows Server 2008 R2.

ETAPE 6. CONFIGURATION DE LA CONNEXION A LA BASE DE DONNEES

Cette étape est disponible uniquement pour l'installation de Kaspersky Anti-Virus sur un serveur autonome ou sur le premier serveur du groupe. Le deuxième serveur et les serveurs suivants utilisent les paramètres indiqués lors de l'installation de l'application sur le premier serveur du groupe.

Vous devez indiquer les paramètres de connexion du module Serveur de sécurité à la base de données dans laquelle seront conservées les informations sur les objets de la sauvegarde et des statistiques du serveur où est installé le module Serveur de sécurité (c'est-à-dire à la *Base de données de la sauvegarde et des statistiques*). Si la Base de données de la sauvegarde et des statistiques n'a pas été créée à l'étape de préparation à l'installation (cf. section "Préparation du serveur SQL" à la page 25), l'Assistant d'installation la créera au moment de l'installation de Kaspersky Anti-Virus.

Dans le champ **Nom du serveur SQL**, saisissez manuellement ou sélectionnez dans la liste des serveurs SQL disponibles, le nom du serveur SQL sur lequel se trouvera la base de données. La liste des serveurs SQL disponibles s'ouvre à l'aide du bouton **Parcourir** (cf. ill. ci-dessous).

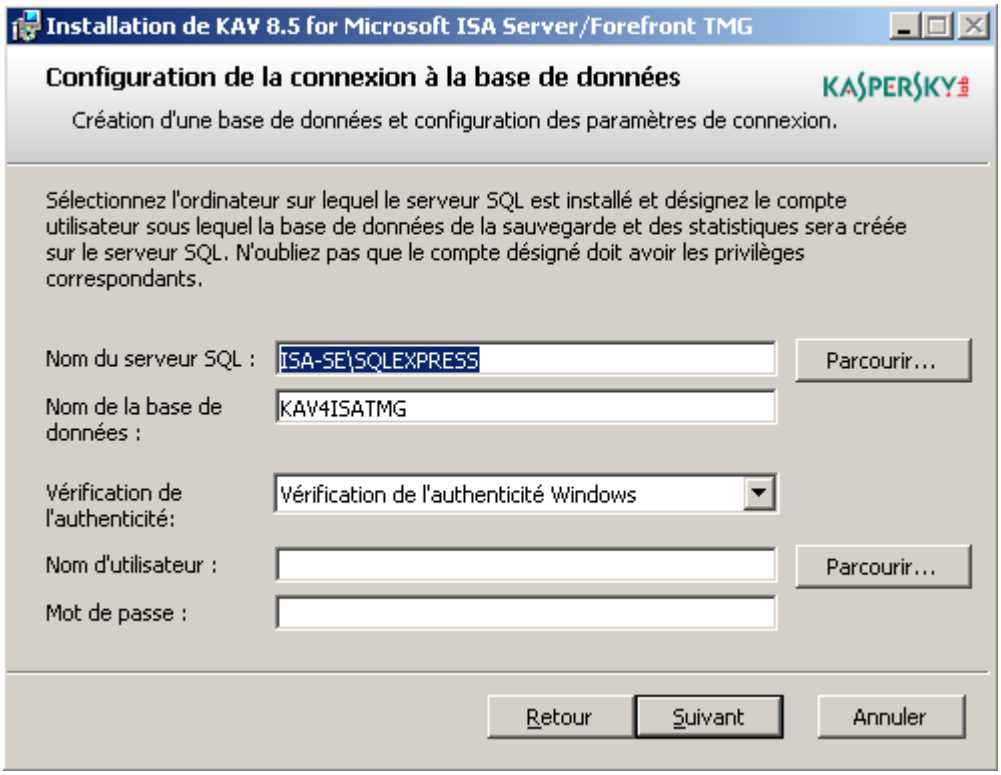

Illustration 6. Configuration de la connexion à la Base de données de la sauvegarde et des statistiques

Dans le champ **Nom de la base de données**, saisissez le nom de la Base de données de la sauvegarde et des statistiques. Vous pouvez indiquer le nom d'une base de données existant sur le serveur SQL existant ou le nom d'une base de données qui sera créée lors de l'installation de l'application.

Par défaut, dans le champ **Nom de la base de données**, la valeur KAV4ISATMG est indiquée.

Sélectionnez le mode d'authentification de l'utilisateur sur le serveur.

- **Vérification de l'authenticité de Windows** : la connexion est effectuée à l'aide du compte utilisateur Windows.
- **Vérification de l'authenticité de SQL** : la connexion est effectuée en vérifiant l'authenticité du serveur SQL.

Dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez l'identifiant et le mot de passe du compte de connexion au serveur SQL et de l'utilisation ultérieure de la Base de données de la sauvegarde et des statistiques :

- Si l'option **Vérification de l'authenticité de Windows** est sélectionnée, saisissez l'identifiant manuellement ou sélectionnez-le dans la liste qui s'ouvre à l'aide du lien **Parcourir**. Saisissez le mot de passe manuellement.
- Si l'option **Vérification de l'authenticité de SQL** est sélectionnée, saisissez l'identifiant et le mot de passe manuellement (le bouton **Parcourir** n'est pas accessible).

Si vous avez créé une base de données à l'étape de préparation de l'installation, vous devez utiliser un compte doté de privilèges d'écriture et d'enregistrement des informations dans la base de données. Si l'Assistant d'installation crée une base de données pendant l'installation de l'application, vous devez utiliser un compte doté de privilèges de création d'une base de données, de déploiement du schéma de la base de données ainsi que de lecture et d'enregistrement des informations dans la base de données. En cas de besoin, vous pouvez modifier les paramètres de connexion à la Base de données de la sauvegarde et des statistiques après l'installation de Kaspersky Anti-Virus dans la Console d'administration de l'application (pour de plus amples informations, cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

L'Assistant d'installation vérifie la présence de la base de données indiquée sur le serveur SQL et la présence pour le compte indiqué des privilèges d'utilisation de cette base de données. Si la base de données indiquée est absente du serveur, l'Assistant d'installation vérifie la présence pour le compte indiqué des privilèges de création d'une base de données, de déploiement du schéma de la base de données et d'utilisation de cette base. Si les privilèges du compte sont insuffisants, l'Assistant d'installation affiche à l'écran un message et le passage à l'étape suivant est impossible.

ETAPE 7. CREATION DE LA REGLE POUR L'ADMINISTRATION A DISTANCE.

Cette étape est disponible uniquement pour l'installation de Kaspersky Anti-Virus sur un serveur autonome ou sur le premier serveur du groupe. Sur le deuxième serveur et sur les serveurs suivants, pour la connexion de la Console d'administration distante au serveur, le numéro de port indiqué lors de l'installation de l'application sur le premier serveur est utilisé.

Au cours de l'installation de Kaspersky Anti-Virus, l'Assistant d'installation crée les règles suivantes :

- la règle ISA/TMG Firewall Policy dans la stratégie du pare-feu du serveur Microsoft ISA Server/Forefront TMG ;
- la règle Windows Firewall (uniquement sur Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2).

Les règles ISA / TMG Firewall Policy et Windows Firewall autorisent les connexions entrantes sur le port de serveur indiqué et permettent d'administration l'application à l'aide de la Console d'administration installée sur un ordinateur distant.

Pour indiquer le port de connexion de la Console d'administration distante au serveur, saisissez le numéro de port dans le champ **Port TCP**.

Le port 5000 est utilisé par défaut. Valeurs possibles : 1026 – 65535.

La règle créée est activée automatiquement, ce qui signifie que l'administration à distance de Kaspersky Anti-Virus est activée.

ETAPE 8. LANCEMENT DE LA COPIE DES FICHIERS ET DE L'ENREGISTREMENT DES MODULES

Une fois les paramètres d'installation configurés, lancez la procédure de copie des fichiers et d'enregistrement des modules de Kaspersky Anti-Virus. Pour ce faire, dans la fenêtre de l'Assistant, cliquez sur le bouton **Installer**.

A l'aide du bouton **Précédent**, vous pouvez retourner aux étapes précédentes d'installation pour consulter et modifier les paramètres d'installation.

ETAPE 9. COPIE DES FICHIERS ET ENREGISTREMENT DES MODULES

A cette étape, l'Assistant d'installation copie les fichiers dans le dossier d'installation de l'application, enregistre les modules de l'application à installer dans le système d'exploitation et les intègre avec le serveur Microsoft ISA Server / Forefront TMG.

Le processus d'installation et d'enregistrement des filtres de Kaspersky Anti-Virus requiert le redémarrage du service Microsoft Firewall. L'Assistant d'installation affiche à l'écran une demande d'arrêt du service.

Pour confirmer l'arrêt du service, cliquez sur le bouton **OK**.

Si vous souhaitez refuser d'arrêter le service, cliquez sur le bouton **Annuler**. L'installation de Kaspersky Anti-Virus sera interrompue et toutes les modifications apportées au système seront supprimées.

ETAPE 10. FIN DE L'INSTALLATION

La fenêtre de l'Assistant affiche un message indiquant que l'installation de Kaspersky Anti-Virus a réussi.

Avant la fin de l'installation de l'application, l'Assistant d'installation supprime tous les objets temporaires et les données qu'il a créées (sauf le journal d'installation) et exécute le lancement du service Microsoft Firewall qu'il avait arrêté au moment de l'installation.

Cliquez sur le bouton **Terminer** pour fermer la fenêtre de l'Assistant d'installation.

Si vous effectuez une installation complète sur un serveur autonome ou sur le premier serveur du groupe juste après la fin de l'Assistant d'installation de Kaspersky Anti-Virus, l'Assistant de configuration initiale de l'application se lance automatiquement (cf. section "Configuration initiale de l'application" à la page 31).

CONFIGURATION INITIALE DE L'APPLICATION

La configuration initiale de Kaspersky Anti-Virus permet juste après l'installation d'activer l'application et de configurer les paramètres de mise à jour des bases de Kaspersky Anti-Virus. La configuration initiale est exécutée après l'installation de l'application sur un serveur autonome ou sur le premier serveur du groupe.

La fenêtre de l'Assistant de configuration initiale s'ouvre automatiquement juste après la fin de l'installation de l'application.

En cas d'utilisation des schémas de déploiement *Groupe autonome* et *Entreprise*, la configuration initiale de Kaspersky Anti-Virus sur le deuxième serveur et sur les serveurs suivants n'est pas requise après l'installation. L'application utilise les paramètres indiqués lors de la configuration initiale sur le premier serveur du groupe ou les paramètres par défaut si vous avez refusé la configuration initiale après l'installation de Kaspersky Anti-Virus sur le premier serveur du groupe.

Toutes les opérations de configuration initiale de l'application sont exécutées dans les fenêtres de l'Assistant de configuration initiale. Pour passer à l'étape suivante de l'Assistant, cliquez sur le bouton **Suivant**. Pour retourner à l'étape précédente de l'Assistant, cliquez sur le bouton **Précédent**. Vous pouvez refuser la configuration initiale de Kaspersky Anti-Virus à n'importe quelle étape de l'Assistant. Pour annuler la configuration initiale de Kaspersky Anti-Virus, cliquez sur le bouton **Annuler**. Si vous avez annulé la configuration initiale de l'application, vous pouvez ensuite activer l'application (cf. section "Activation de l'application" à la page 38) et configurer les paramètres de mise à jour des bases de Kaspersky Anti-Virus à l'aide de la Console d'administration de l'application (pour de plus amples informations, cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

La fenêtre de l'Assistant de configuration initiale s'ouvre automatiquement juste après la fin de l'installation de l'application.

DANS CETTE SECTION

Etape 1. Activation de l'application 32

Etape 2. Configuration des paramètres de mise à jour 32

ETAPE 1. ACTIVATION DE L'APPLICATION

A la première étape de l'Assistant de configuration initiale, vous pouvez activer l'application. Pour ce faire, vous devez ajouter la clé. Si l'application n'est pas activée, seule l'administration de Kaspersky Anti-Virus est disponible. L'analyse du trafic et la mise à jour des bases antivirus ne sont pas effectuées.

Cliquez sur le bouton **Ajouter** et dans la fenêtre qui s'ouvre, sélectionnez le fichier clé (fichier avec l'extension key). La clé ajoutée devient active (Pour de plus amples informations sur les clés, cf. *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*. Les informations sur la clé ajoutée s'affichent dans la fenêtre de l'Assistant.

En cas d'utilisation du schéma de déploiement *Entreprise*, lors de la configuration initiale de Kaspersky Anti-Virus sur le premier serveur du deuxième groupe et des groupes suivants de l'entreprise, la fenêtre de l'Assistant affiche les informations sur la clé ajoutée sur le premier serveur du premier groupe. Vous pouvez remplacer cette clé à l'aide du bouton **Remplacer** dans la fenêtre de l'Assistant.

ETAPE 2. CONFIGURATION DES PARAMETRES DE MISE A JOUR

A la deuxième étape de l'Assistant de configuration initiale, vous pouvez configurer les paramètres de mise à jour des bases de Kaspersky Anti-Virus.

La case **Mettre à jour les bases de Kaspersky Anti-Virus par programmation** permet de configurer le lancement de la mise à jour des bases de Kaspersky Anti-Virus toutes les heures. Par défaut, la case **Mettre à jour les bases de Kaspersky Anti-Virus par programmation** est cochée. Si vous souhaitez désactiver le lancement de la mise à jour programmée, décochez la case.

Si la connexion au serveur de mise à jour des bases de Kaspersky Anti-Virus utilise un serveur proxy, configurez-en les paramètres dans la fenêtre **Serveur proxy** qui s'ouvre à l'aide du bouton **Serveur proxy**. Cochez la case **Utiliser le serveur proxy** et effectuez une des actions suivantes :

- Si le serveur proxy de Microsoft ISA Server / Forefront TMG est utilisé pour accéder à la source de mise à jour, sélectionnez l'option **Serveur proxy local**.
- Si un autre serveur proxy est utilisé pour accéder à la source de mise à jour, sélectionnez l'option **Serveur proxy distant**. Dans les champs **Adresse** et **Port**, indiquez l'adresse IP et le numéro de port réseau du serveur proxy.

Si le serveur proxy servant à se connecter à la source de mise à jour utilise la vérification de l'authenticité, cochez la case **Vérification de l'authenticité nécessaire** et indiquez le **Nom de l'utilisateur** et le **Mot de passe**.

Fermez la fenêtre **Serveur proxy** en cliquant sur le bouton **OK**.

Cliquez sur le bouton **Terminer** pour fermer la fenêtre de l'Assistant de configuration initiale de l'application.

Une fois l'Assistant de configuration initiale terminé, la Console d'administration de Kaspersky Anti-Virus se lance automatiquement. Pour commencer à utiliser l'application, vous devez vous connecter à la Console d'administration du stockage de configuration de Microsoft ISA Server / Forefront TMG. (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35)

INSTALLATION DE LA CONSOLE D'ADMINISTRATION

Cette section décrit l'installation de la Console d'administration de Kaspersky Anti-Virus sur l'ordinateur à l'aide de l'Assistant d'installation.

Vous pouvez installer la Console d'administration sur un ordinateur séparé ayant accès via le réseau au serveur où est installé le module Serveur de sécurité.

La présence de la console Microsoft ISA Server/Forefront TMG installée sur l'ordinateur est une exigence indispensable pour installer la Console d'administration de Kaspersky Anti-Virus.

Avant de commencer à installer la Console d'administration, installez sur l'ordinateur les applications complémentaires nécessaires à l'installation et au fonctionnement de la Console d'administration (cf. section "Installation d'applications complémentaires" à la page 24) et assurez-vous que des versions antérieures de Kaspersky Anti-Virus et que d'autres applications antivirus pour Microsoft ISA Server / Forefront TMG ne sont pas installées sur l'ordinateur.

DANS CETTE SECTION

Etape 1. Début de l'installation 33

Etape 2. Confirmation du Contrat de licence 33

Etape 3. Sélection du type d'installation 34

Etape 4. Sélection du dossier d'installation 34

Etape 5. Lancement de la copie des fichiers et de l'enregistrement des modules 35

Etape 6. Copie des fichiers et enregistrement des modules 35

Etape 7. Fin de l'installation 35

ETAPE 1. DEBUT DE L'INSTALLATION

Pour commencer l'installation de la Console d'administration de Kaspersky Anti-Virus, lancez le fichier exécutable kav4isa_8.5.XXXX_ee_ru.exe (où XXXX est le numéro de version) faisant partie de la distribution.

La fenêtre de l'Assistant d'installation s'ouvre.

Si l'Assistant d'installation détecte sur l'ordinateur une version antérieure de Kaspersky Anti-Virus for Microsoft ISA Server / Forefront TMG, l'écran affiche un message et l'Assistant d'installation se termine.

L'Assistant d'installation vérifie la présence sur l'ordinateur des applications complémentaires nécessaires à l'installation et au fonctionnement de la Console d'administration de Kaspersky Anti-Virus (cf. section "Installation d'applications complémentaires" à la page 24).

Si des applications complémentaires nécessaires manquent, l'écran affiche un message et l'Assistant d'installation se termine. Installez les applications complémentaires nécessaires et relancez l'Assistant d'installation de Kaspersky Anti-Virus.

ETAPE 2. CONFIRMATION DU CONTRAT DE LICENCE

Lisez le Contrat de licence. Pour poursuivre l'installation, vous devez accepter les conditions du contrat.

Pour accepter les conditions du Contrat de licence, cochez la case **J'accepte les conditions du Contrat de licence**.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Cliquez sur le bouton **Console d'administration** pour installer sur l'ordinateur uniquement le module Console d'administration de Kaspersky Anti-Virus.

Le bouton **Console d'administration** est inaccessible si la configuration matérielle et logicielle de l'ordinateur ne correspond pas aux exigences de Kaspersky Anti-Virus (cf. section "Configurations matérielles et logicielles" à la page 11).

ETAPE 4. SELECTION DU DOSSIER D'INSTALLATION

Vous devez indiquer le dossier dans lequel sera installé la Console d'administration de Kaspersky Anti-Virus.

Pour indiquer le dossier dans lequel sera installé la Console d'administration, cliquez sur le bouton **Parcourir** (cf. ill. ci-dessous). Dans la fenêtre qui s'ouvre, sélectionnez le dossier ou saisissez le chemin du dossier manuellement.

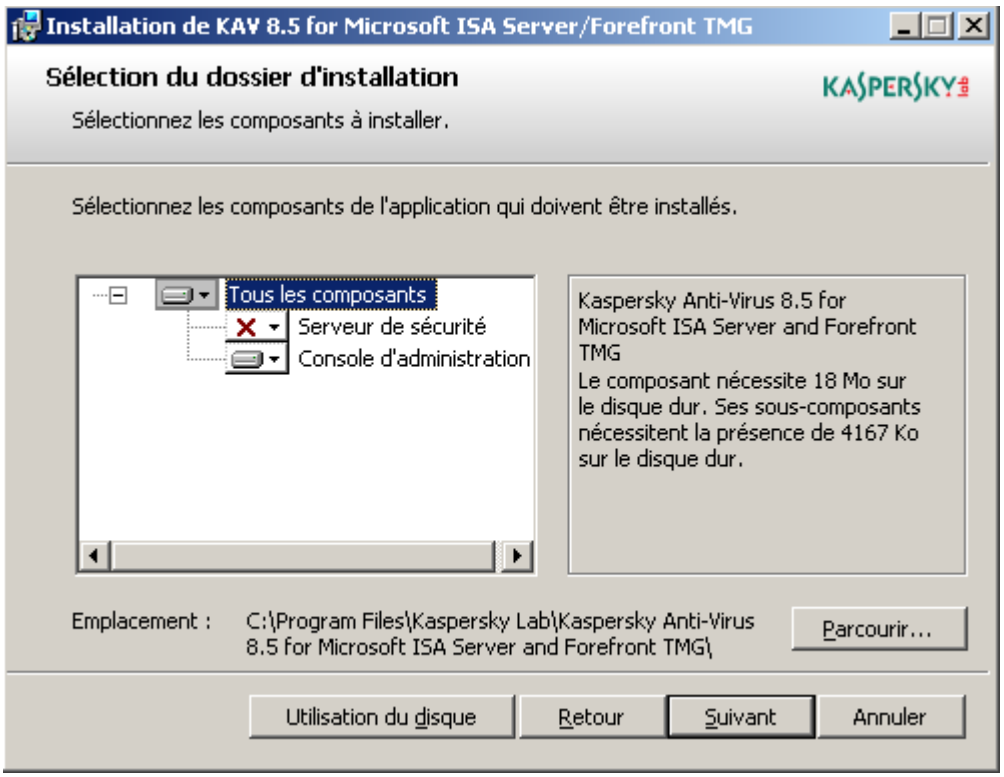

Illustration 7. Sélection du dossier d'installation : installation de la Console d'administration

Si vous avez indiqué un dossier inexistant, l'Assistant créera le dossier avec le nom indiqué.

Par défaut, la Console d'administration de Kaspersky Anti-Virus est installée dans le dossier <ProgramFiles>\Kaspersky Lab\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG, où <ProgramFiles> peut avoir l'une des valeurs suivantes :

- %ProgramFiles% (sous un système d'exploitation 32-bits) ou %ProgramFiles(x86)% (sous un système d'exploitation 64-bits) si Microsoft ISA Server / Forefront TMG est installé sur le même disque que le système d'exploitation Microsoft Windows;
- <Disque avec Microsoft ISA Server / Forefront TMG>:\Program Files : si Microsoft ISA Server / Forefront TMG et le système d'exploitation Microsoft Windows sont installés sur des disques différents.

ETAPE 5. LANCEMENT DE LA COPIE DES FICHIERS ET DE L'ENREGISTREMENT DES MODULES

Une fois la configuration des paramètres de l'installation terminée, lancez la procédure de copie des fichiers et d'enregistrement du module Console d'administration de Kaspersky Anti-Virus. Pour ce faire, dans la fenêtre de l'Assistant, cliquez sur le bouton **Installer**.

A l'aide du bouton **Précédent**, vous pouvez retourner aux étapes précédentes d'installation pour consulter et modifier les paramètres d'installation.

ETAPE 6. COPIE DES FICHIERS ET ENREGISTREMENT DES MODULES

A cette étape, l'Assistant d'installation copie les fichiers dans le dossier d'installation et enregistre la Console d'administration de Kaspersky Anti-Virus dans le système d'exploitation.

ETAPE 7. FIN DE L'INSTALLATION

La fenêtre de l'Assistant affiche un message indiquant que l'installation de la Console d'administration de Kaspersky Anti-Virus a réussi.

Cliquez sur le bouton **Terminer** pour fermer la fenêtre de l'Assistant d'installation.

CONNEXION DE LA CONSOLE D'ADMINISTRATION AU STOCKAGE DE CONFIGURATION

La Console d'administration de Kaspersky Anti-Virus assure l'administration par Kaspersky Anti-Virus. Pour commencer à utiliser l'application, vous devez vous connecter à la Console d'administration du stockage de configuration de Microsoft ISA Server / Forefront TMG.

DANS CETTE SECTION

Actions préalables avant la connexion de la Console d'administration 35

Connexion au stockage de configuration 36

ACTIONS PREALABLES AVANT LA CONNEXION DE LA CONSOLE D'ADMINISTRATION

Pour connecter la Console d'administration de Kaspersky Anti-Virus au stockage de configuration de Microsoft ISA Server/Forefront TMG, vous pouvez utiliser le compte Microsoft Windows sous lequel la Console d'administration a été lancée (c'est-à-dire le compte actuel) ou un autre compte indiqué lors de la connexion.

Le compte sous lequel la connexion au stockage de configuration Microsoft ISA Server/Forefront TMG a lieu, doit posséder les privilèges de consultation ou de lecture/enregistrement de la configuration de Kaspersky Anti-Virus (cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

Pour obtenir l'accès au service *Kaspersky Anti-Virus 8.5 for ISA Server and Forefront TMG* (kavisasrv.exe), assurant le fonctionnement de Kaspersky Anti-Virus, le compte de l'utilisateur doit faire partie d'un des groupes suivants d'utilisateurs du système d'exploitation Windows : Utilisateurs DCOM (Distributed COM Users), Administrateurs du domaine ou groupe des administrateurs locaux.

Le compte, sous lequel la connexion au stockage de configuration a lieu, est aussi utilisé lors de la connexion de la Console d'administration à la Base de données de la sauvegarde et des statistiques. Pour pouvoir utiliser les objets de la Sauvegarde, assurez-vous que le compte, sous lequel la connexion a lieu, possède les privilèges de lecture et d'enregistrement des informations dans la Base de données de la sauvegarde et des statistiques.

En cas de déploiement de Kaspersky Anti-Virus dans le groupe de travail, il faut assurer également la possibilité de connexion à la Base de données de la sauvegarde et des statistiques. Pour ce faire, procédez comme suit :

1. Sur le serveur physique sur lequel le système d'administration de la base de données Microsoft SQL Server est installé avec la Base de données de la sauvegarde et des statistiques, créer un compte, via les outils du système d'exploitation Microsoft Windows, identique au compte sous lequel la Console d'administration de Kaspersky Anti-Virus se lance.

2. Configurer pour le compte créé les privilèges nécessaires d'accès à la Base de données de la sauvegarde et des statistiques via les outils du système d'administration de la base de données Microsoft SQL Server.

CONNEXION AU STOCKAGE DE CONFIGURATION

Pour connecter la Console d'administration de Kaspersky Anti-Virus au stockage de configuration Microsoft ISA Server/Forefront TMG, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Anti-Virus.

   La fenêtre **Connexion au serveur du stockage de configuration** (cf. ill. ci-après) s'ouvre.

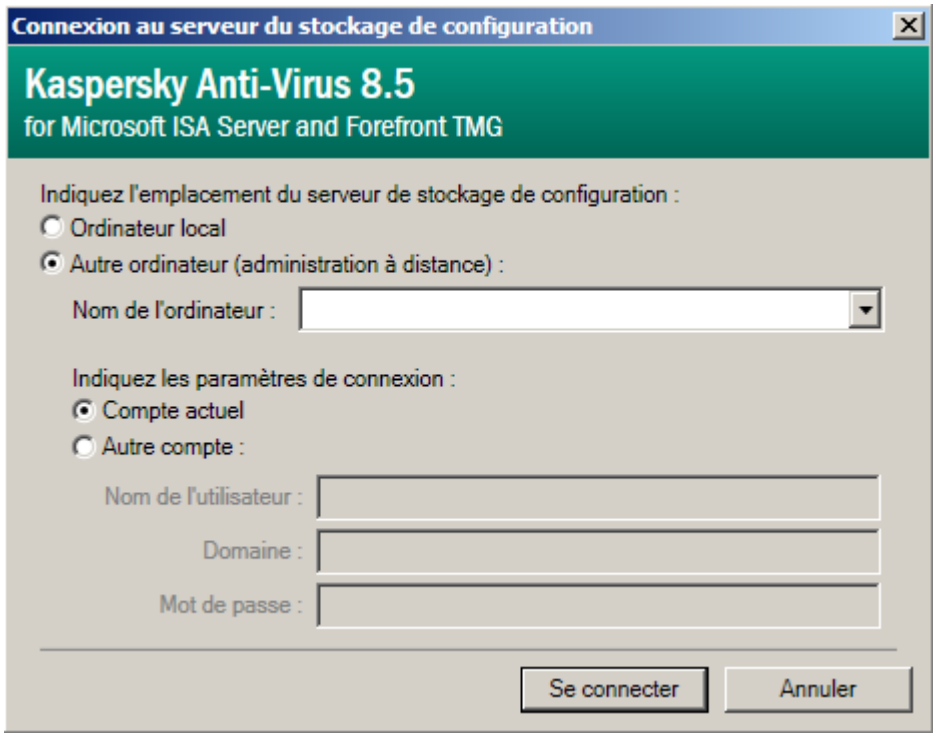

*Illustration 8. Fenêtre **Connexion au serveur du stockage de configuration***

Si auparavant la Console d'administration s'est connectée avec succès au stockage de configuration, la fenêtre affiche tous les paramètres de la dernière connexion réussie, sauf le mot de passe de l'utilisateur.

2. Sélectionnez l'option d'emplacement du stockage de configuration :

   - **Ordinateur local**

     La Console d'administration de Kaspersky Anti-Virus se connecte au stockage de configuration situé sur le même ordinateur sur lequel la Console d'administration a été lancée.

     Cette valeur est sélectionnée par défaut si auparavant la Console d'administration ne se connectait pas au stockage de configuration. Si la connexion est réitérée, la fenêtre affiche les paramètres de la dernière connexion réussie.

   - **Autre ordinateur (administration à distance)**

     La Console d'administration de Kaspersky Anti-Virus se connecte au stockage de configuration situé sur un autre ordinateur.

     Utilisez cette option de connexion s'il faut effectuer l'administration à distance de Kaspersky Anti-Virus. Dans ce cas, il faut définir les paramètres de connexion et le nom/l'adresse IP de l'ordinateur sur lequel le stockage de configuration se trouve.

3. Si le stockage de configuration est situé sur un ordinateur distant, indiquez les paramètres de connexion suivants :

   - **Nom de l'ordinateur**

     Nom et adresse IP de l'ordinateur sur lequel la connexion a lieu.

     Si la connexion de la Console d'administration au stockage de configuration est exécutée pour la première fois, il faut indiquer l'adresse IP dans ce champ, ainsi que le nom de l'ordinateur (si l'ordinateur fait partie du domaine, il faut indiquer le nom complet du domaine) ou le nom NetBIOS de l'ordinateur sur lequel le stockage de configuration se trouve.

     Kaspersky Anti-Virus enregistre les paramètres de la précédente connexion réussie de la Console d'administration au stockage de configuration. Si une nouvelle connexion de la Console d'administration au stockage de configuration est exécutée, la liste déroulante permet de sélectionner le nom de l'ordinateur auquel la connexion avait réussi.

   - Compte pour la connexion :

     - **Compte actuel**

       La Console d'administration utilise le compte actuel (c'est-à-dire le compte Microsoft Windows sous lequel la Console d'administration est lancée) pour se connecter au stockage de configuration.

       Ce paramètre est sélectionné par défaut si auparavant la Console d'administration ne se connectait pas au stockage de configuration. Si la connexion est réitérée, la fenêtre affiche les paramètres de la dernière connexion réussie.

     - **Autre compte**

       La Console d'administration utilise un compte Microsoft Windows différent du compte actuel pour se connecter au stockage de configuration.

       En cas de sélection de cette option, il faut indiquer le nom d'utilisateur, le mot de passe du compte et le nom de domaine dans lequel le compte est enregistré (si l'ordinateur sur lequel le stockage de configuration se trouve fait partie du domaine).

4. Si vous exécutez la connexion à un ordinateur distant avec un compte différent du compte actuel, indiquez la valeur des paramètres **Nom de l'utilisateur** et **Mot de passe**. Si l'ordinateur sur lequel se trouve le stockage de configuration fait partie du domaine, saisissez aussi la valeur du champ **Domaine**.

   Si le compte, sous lequel la connexion a lieu, ne possède pas assez de privilèges pour se connecter au stockage de configuration, Kaspersky Anti-Virus affiche sur l'écran un message relatif à cet événement.

5. Cliquez sur le bouton **Connexion**.

Suite à la connexion de la Console d'administration au stockage de configuration, l'arborescence de la console affiche les entrées prévues pour travailler avec les paramètres de Kaspersky Anti-Virus. La composition des entrées dans l'arborescence de la console dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé (cf. section "Schémas types de déploiement de l'application" à la page 17) et du rôle de l'utilisateur sous le compte duquel la connexion de la Console d'administration au stockage de configuration a eu lieu (cf. le *Manuel de l'administrateur de "Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG"*).

Si la connexion de la Console d'administration au stockage de configuration n'est pas établie (par exemple, une erreur s'est produite lors de la connexion), l'arborescence de la console contient uniquement l'entrée racine **Kaspersky Anti-Virus**. Vous pouvez établir la connexion à l'aide du bouton **Connexion** situé dans le panneau des résultats de l'entrée **Kaspersky Anti-Virus.**

ACTIVATION DE L'APPLICATION

Avant de commencer à utiliser Kaspersky Anti-Virus, il faut activer l'application si elle n'a pas été activée juste après l'installation (cf. section "Configuration initiale de l'application" à la page 31).

Si l'application n'est pas activée, seule l'administration de Kaspersky Anti-Virus est disponible. L'analyse du trafic et la mise à jour des bases antivirus ne sont pas effectuées.

Pour activer l'application, il faut ajouter une clé. Pour ce faire, il faut utiliser le fichier clé.

Kaspersky Anti-Virus permet d'ajouter deux clés. La clé ajoutée en premier devient une clé *active.* La présence de la clé active assure la fonctionnalité complète de l'application. La deuxième clé devient une clé supplémentaire. La *clé supplémentaire* devient une clé active soit à l'expiration de la clé active, soit lors de la suppression de la clé active. La présence de la clé supplémentaire permet d'éviter les restrictions de fonctionnalité de l'application au moment de l'expiration de la licence. Pour de plus amples informations sur les clés cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*.

Pour ajouter une clé active ou supplémentaire, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35).
2. Exécutez une des actions suivantes :
   - Si le schéma de déploiement utilisé est *Entreprise*, déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Licence**.
   - Si le schéma de déploiement utilisé est *Serveur autonome* ou *Groupe autonome*, déployez l'entrée du serveur/du groupe et sélectionnez l'entrée jointe **Licence**.
3. Dans le panneau des résultats, cliquez sur le bouton **Ajouter**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier clé (fichier avec l'extension key).

   La clé supplémentaire doit satisfaire les conditions suivantes : ne pas être ajoutée en tant que clé active et ne doit pas expirer avant la clé active. Si la clé ne satisfait pas les conditions indiquées, un message d'erreur s'affiche. Il n'est pas recommandé d'utiliser la clé de la version d'essai comme clé supplémentaire.

5. Pour que les modifications entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale. La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Les informations sur la clé ajoutée seront affichées dans le panneau des résultats de l'entrée **Licence** (pour de amples renseignements, cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

MODIFICATIONS DANS LE SYSTEME APRES L'INSTALLATION DE L'APPLICATION

Au moment de l'installation de l'application, l'Assistant d'installation crée les dossiers suivants :

- Dossier d'installation. Par défaut, Kaspersky Anti-Virus est installé dans le dossier <ProgramFiles>\Kaspersky Lab\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG, où <ProgramFiles> peut avoir l'une des valeurs suivantes :
  - %ProgramFiles% (sous un système d'exploitation 32-bits) ou %ProgramFiles(x86)% (sous un système d'exploitation 64-bits) : si le serveur proxy de Microsoft ISA Server / Forefront TMG est installé sur le même disque que le système d'exploitation Microsoft Windows ;
  - <Disque avec Microsoft ISA Server / Forefront TMG>:\Program Files : si le serveur proxy de Microsoft ISA Server / Forefront TMG et le système d'exploitation Microsoft Windows sont installés sur des disques différents.
- Dossier de conservation des données. Par défaut, pour conserver les données créées pendant le fonctionnement de l'application, le dossier <CommonAppDataFolder>\Kaspersky Lab\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG\data est utilisé, où <CommonAppDataFolder> peut avoir l'une des valeurs suivantes :
  - %AllUsersProfile%\Application Data : si vous installez l'application sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows XP ou Microsoft Windows Server 2003 ;
  - %ProgramData% : si vous installez l'application sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows Server 2008 ou Microsoft Windows Server 2008 R2.

  La valeur <CommonAppDataFolder> se trouve dans la clé de registre [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders].
- Dossier des composants partagés (ISD): <CommonFilesFolder>\Kaspersky Lab\ISD.

  Le chemin du dossier est enregistré dans l'une des variables système suivantes :
  - %CommonProgramFiles% si l'application est installée sous un système d'exploitation 32-bits ;
  - %CommonProgramFiles(x86)% si l'application est installée sous un système d'exploitation 64-bits.

  La valeur <CommonFilesFolder> se trouve dans l'une des clés de registre suivantes :
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir] si l'application est installée sous un système d'exploitation 32-bits ;
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir (x86)] si l'application est installée sous un système d'exploitation 64-bits.
- Dossier dans le menu **Démarrer** : <ProgramMenuFolder>\Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG, où <ProgramMenuFolder> est le dossier contenant les éléments du menu **Démarrer** pour tous les utilisateurs.

  La valeur <ProgramMenuFolder> se trouve dans la clé de registre [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders].

Au cours de l'installation, l'Assistant d'installation effectue également les actions suivantes :

- Enregistre dans le système le service *Kaspersky Anti-Virus 8.5 for ISA Server et Forefront TMG* (kavisasrv.exe).
- Crée dans la stratégie du pare-feu du serveur Microsoft ISA Server / Forefront TMG la règle ISA / TMG Firewall Policy qui autorise l'accès à distance de la Console d'administration à l'ordinateur sur lequel Kaspersky Anti-Virus est installé.

- Sous les systèmes d'exploitation Windows Server 2008 et Windows Server 2008 R2, crée la règle Windows Firewall pour le pare-feu qui autorise l'accès de la Console d'administration à l'ordinateur sur lequel Kaspersky Anti-Virus est installé.
- Ajoute deux groupes de compteurs de performance : *Filtres de Kav for ISA and TMG* et *Service de Kav for ISA and TMG.*
- Enregistre le mécanisme de notification des évènements de Kaspersky Anti-Virus dans Microsoft ISA Server/Forefront TMG.

DEPLACEMENT DES SERVEURS FOREFRONT TMG AVEC KASPERSKY ANTI-VIRUS

La possibilité d'ajouter le serveur au groupe autonome inclus dans l'entreprise, ainsi que d'exclure du groupe/de l'entreprise est proposée dans Microsoft Forefront TMG.

Selon le schéma de déploiement, la configuration de Kaspersky Anti-Virus sur le serveur se compose de deux ou de trois niveaux logiques (cf. section "Configuration de Kaspersky Anti-Virus" à la page 14). Lors de l'ajout du serveur au groupe/à l'entreprise ou lors de l'exclusion du serveur du groupe/de l'entreprise, les paramètres au niveau du serveur restent inchangés. Les paramètres au niveau du groupe et de l'entreprise sont remplacés par les paramètres du stockage de configuration Microsoft ISA Server/Forefront TMG du groupe/de l'entreprise auquel/à laquelle s'ajoute le serveur. Ainsi, suite à l'ajout du serveur avec Kaspersky Anti-Virus installé au groupe/à l'entreprise ou à son exclusion du groupe/de l'entreprise, l'intégrité de la configuration de l'application peut être perturbée. En cas de perturbation de la configuration, Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

Cette section décrit les perturbations possibles de l'intégrité de la configuration de Kaspersky Anti-Virus qui apparaissent suite au déplacement des serveurs, ainsi que les recommandations de restauration du fonctionnement de l'application.

Les opérations types suivantes de déplacement des serveurs Forefront TMG EE/SE avec Kaspersky Anti-Virus installé sont examinées :

- Ajout du serveur Forefront TMG EE à un groupe autonome
- Ajout du serveur Forefront TMG EE au groupe existant sous l'administration de EMS
- Ajout du serveur Forefront TMG EE faisant partie du nouveau groupe à l'entreprise
- Ajout du serveur Forefront TMG SE à l'entreprise
- Exclusion du serveur Forefront TMG EE/SE du groupe autonome ou du groupe faisant partie de l'entreprise.

DANS CETTE SECTION

Ajout du serveur Forefront TMG EE au groupe autonome 41

Ajout du serveur Forefront TMG EE au groupe existant sous l'administration de EMS 41

Ajout du serveur Forefront TMG EE faisant partie du nouveau groupe à l'entreprise 42

Ajout du serveur Forefront TMG SE à l'entreprise 43

Exclusion du serveur du groupe ou de l'entreprise 44

Restauration de la configuration de Kaspersky Anti-Virus 44

AJOUT DU SERVEUR FOREFRONT TMG EE AU GROUPE AUTONOME

Avant l'ajout du serveur au groupe autonome, les paramètres de Kaspersky Anti-Virus au niveau du serveur et au niveau du groupe sont présents dans le stockage de configuration du serveur. Après l'ajout au groupe, le serveur utilisera les paramètres au niveau du groupe enregistrés dans le stockage de configuration du groupe.

Le fonctionnement de Kaspersky Anti-Virus sur le serveur, ajouté au groupe, dépend de la présence de la configuration correcte de l'application au niveau du groupe dans le stockage de configuration du groupe :

- Si le stockage de configuration du groupe possède une configuration correcte de Kaspersky Anti-Virus, l'application est opérationnelle sur le serveur car la configuration de l'application sur le serveur se compose comme d'habitude de deux niveaux logiques (niveau du serveur et niveau du groupe).

  Les paramètres de Kaspersky Anti-Virus au niveau du serveur restent inchangés ; les paramètres généraux pour tous les serveurs du groupe sont appliqués au niveau du groupe. Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

- Si Kaspersky Anti-Virus n'est pas configuré ou mal configuré dans le stockage de configuration du groupe, Kaspersky Anti-Virus n'est pas opérationnel sur le serveur car le stockage de configuration possède uniquement une configuration correcte au niveau du serveur.

  En cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration du groupe, les paramètres par défaut de Kaspersky Anti-Virus au niveau du groupe sont enregistrés dans le stockage de configuration.

En cas de déploiement de Kaspersky Anti-Virus dans un groupe de serveurs, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

AJOUT DU SERVEUR FOREFRONT TMG EE AU GROUPE EXISTANT SOUS L'ADMINISTRATION DE EMS

Avant l'ajout du serveur au groupe sous l'administration EMS, les paramètres de Kaspersky Anti-Virus au niveau du serveur et au niveau du groupe sont présents dans le stockage de configuration du serveur. Après l'ajout au groupe, le serveur utilisera les paramètres au niveau du groupe et au niveau de l'entreprise enregistrés dans le stockage de configuration de l'entreprise.

Le fonctionnement de Kaspersky Anti-Virus sur le serveur, ajouté au groupe, dépend de la présence de la configuration correcte de l'application au niveau du groupe et au niveau de l'entreprise dans le stockage de configuration de l'entreprise :

- Si le stockage de configuration de l'entreprise possède une configuration correcte de Kaspersky Anti-Virus, l'application n'est pas opérationnelle sur le serveur car la configuration de l'application sur le serveur se compose de trois niveaux logiques (niveau du serveur, niveau du groupe et niveau de l'entreprise).

  Les paramètres de Kaspersky Anti-Virus au niveau du serveur restent inchangés ; les paramètres généraux pour tous les serveurs du groupe et de l'entreprise sont appliqués au niveau du groupe et de l'entreprise. Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

- Si Kaspersky Anti-Virus n'est pas configuré ou mal configuré au niveau du groupe ou au niveau de l'entreprise dans le stockage de configuration de l'entreprise, Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

  En cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration de l'entreprise, les paramètres suivants par défaut de Kaspersky Anti-Virus sont enregistrés dans le stockage de configuration :

- les paramètres au niveau du groupe, si la configuration de Kaspersky Anti-Virus au niveau du groupe n'est pas correcte ou est absente du stockage de configuration ;
- les paramètres au niveau de l'entreprise et au niveau du groupe, si la configuration de Kaspersky Anti-Virus au niveau de l'entreprise et au niveau du groupe n'est pas correcte ou est absente du stockage de configuration.

En cas de déploiement de Kaspersky Anti-Virus dans un groupe de serveurs, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

AJOUT DU SERVEUR FOREFRONT TMG EE FAISANT PARTIE DU NOUVEAU GROUPE A L'ENTREPRISE

Le serveur Forefront TMG EE peut être ajouté à l'entreprise faisant partie du nouveau groupe. Les options suivantes de formation de la configuration du nouveau groupe sont prévues :

- création de la configuration du groupe à partir de la configuration du serveur ;
- création de la configuration du groupe à partir de de la configuration par défaut.

Avant l'ajout à l'entreprise, les paramètres de Kaspersky Anti-Virus au niveau du serveur et au niveau du groupe sont présents dans le stockage de configuration du serveur.

Configuration du groupe à partir de la configuration du serveur

Si la configuration du nouveau groupe (incluant le serveur qui est ajouté à l'entreprise) est créée à partir de la configuration de ce serveur, après l'ajout du serveur à l'entreprise, les paramètres de Kaspersky Anti-Virus au niveau du serveur et au niveau du groupe sont présents dans le stockage de configuration de l'entreprise.

Le fonctionnement de Kaspersky Anti-Virus sur le serveur, après l'ajout au serveur de l'entreprise, dépend de la présence de la configuration correcte de l'application au niveau de l'entreprise dans le stockage de configuration de l'entreprise.

- Si une configuration correcte de Kaspersky Anti-Virus au niveau de l'entreprise existe dans le stockage de configuration de l'entreprise, l'application est opérationnelle sur le serveur.

  Le serveur utilisera les paramètres au niveau de l'entreprise enregistrés dans le stockage de configuration.

- Si la configuration au niveau de l'entreprise est incorrecte ou absente dans le stockage de configuration, Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

  En cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration de l'entreprise, les paramètres par défaut de Kaspersky Anti-Virus au niveau de l'entreprise et au niveau du groupe sont enregistrés dans le stockage de configuration.

Configuration du groupe à partir de la configuration par défaut.

Si la configuration du nouveau groupe pour lequel le serveur est ajouté à l'entreprise, est créée à partir de la configuration par défaut, la configuration au niveau du groupe est remplacée par la configuration par défaut suite à l'ajout du serveur à l'entreprise. Les paramètres de Kaspersky Anti-Virus au niveau du groupe sont absents du stockage de configuration.

Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

- Si la configuration au niveau de l'entreprise est incorrecte ou absente dans le stockage de configuration, en cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

- Si le stockage de configuration de l'entreprise possède une configuration correcte de Kaspersky Anti-Virus au niveau de l'entreprise, la Console d'administration n'affiche pas l'entrée du nouveau groupe dont fait partie le serveur qui est ajouté à l'entreprise.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration de l'entreprise, les paramètres suivants par défaut de Kaspersky Anti-Virus sont enregistrés dans le stockage de configuration :

- les paramètres au niveau du groupe pour le nouveau groupe dont fait partie le serveur qui est ajouté à l'entreprise, si le stockage de configuration possède une configuration correcte de Kaspersky Anti-Virus au niveau de l'entreprise ;

- les paramètres au niveau de l'entreprise et au niveau du groupe, si Kaspersky Anti-Virus au niveau de l'entreprise n'est pas configuré ou mal configuré dans le stockage de configuration.

AJOUT DU SERVEUR FOREFRONT TMG SE A L'ENTREPRISE

Le serveur Forefront TMG SE peut être ajouté à l'entreprise uniquement pour faire partie du nouveau groupe. La configuration du nouveau groupe est formée à partir de la configuration par défaut.

Avant l'ajout au groupe, les paramètres de Kaspersky Anti-Virus au niveau du serveur et au niveau du groupe sont présents dans le stockage de configuration du serveur. Suite à l'ajout du serveur à l'entreprise, la configuration au niveau du groupe est remplacée par la configuration par défaut. Les paramètres de Kaspersky Anti-Virus au niveau du groupe sont absents du stockage de configuration.

Kaspersky Anti-Virus n'est pas opérationnel sur le serveur.

- Si la configuration au niveau de l'entreprise est incorrecte ou absente dans le stockage de configuration, en cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

- Si le stockage de configuration de l'entreprise possède une configuration correcte de Kaspersky Anti-Virus au niveau de l'entreprise, la Console d'administration n'affiche pas l'entrée du nouveau groupe dont fait partie le serveur qui est ajouté à l'entreprise.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration de l'entreprise, les paramètres suivants par défaut de Kaspersky Anti-Virus sont enregistrés dans le stockage de configuration :

- les paramètres au niveau du groupe pour le nouveau groupe dont fait partie le serveur qui est ajouté à l'entreprise, si le stockage de configuration possède une configuration correcte de Kaspersky Anti-Virus au niveau de l'entreprise ;

- les paramètres au niveau de l'entreprise et au niveau du groupe, si Kaspersky Anti-Virus au niveau de l'entreprise n'est pas configuré ou mal configuré dans le stockage de configuration.

EXCLUSION DU SERVEUR DU GROUPE OU DE L'ENTREPRISE

Le serveur sur lequel est installé Kaspersky Anti-Virus peut être exclu du groupe autonome ou du groupe de l'entreprise.

La configuration de Kaspersky Anti-Virus sur le serveur, faisant partie du groupe ou de l'entreprise, se compose de deux (pour le groupe) ou de trois (pour l'entreprise) niveaux logiques. Après l'exclusion du serveur du groupe ou de l'entreprise, seuls les paramètres de l'application au niveau du serveur restent dans le stockage de configuration du serveur. Kaspersky Anti-Virus n'est pas opérationnel sur le serveur. En cas de tentative de connexion de la Console d'administration au stockage de configuration de Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 35), Kaspersky Anti-Virus affiche un message indiquant que la configuration de l'application est introuvable.

Pour restaurer le fonctionnement de Kaspersky Anti-Virus, il faut exécuter une restauration de la configuration de l'application sur le serveur (cf. section "Restauration de la configuration de Kaspersky Anti-Virus" à la page 44).

Suite à la restauration du serveur, les paramètres par défaut de Kaspersky Anti-Virus au niveau du groupe sont enregistrés dans le stockage de configuration.

RESTAURATION DE LA CONFIGURATION DE KASPERSKY ANTI-VIRUS

Pour restaurer le fonctionnement de Kaspersky Anti-Virus sur le serveur, procédez comme suit :

1. Lancez l'utilitaire de restauration de la configuration ConfigurationRepairTool.exe dans la ligne de commande sur le serveur.

   L'utilitaire de restauration vérifie l'intégrité de la configuration de Kaspersky Anti-Virus dans le stockage de configuration.

   Si la configuration de l'application est absente ou corrompue, l'utilitaire demande les paramètres nécessaires à la restauration de la configuration.

2. Si besoin, indiquez les paramètres suivants :

   - Numéro de port de connexion de la Console d'administration distante au serveur pour la règle ISA/TMG Firewall Policy (par exemple, 5000).
   - Nom du serveur SQL sur lequel se trouve la Base de données de la sauvegarde et des statistiques (par exemple Server\SQLExpress).
   - Nom de la Base de données de la sauvegarde et des statistiques (par exemple, kav4isatmg).
   - Mode d'authentification de l'utilisateur sur le serveur SQL (1, si la connexion est exécutée à l'aide d'un compte utilisateur Windows, ou 2, si la connexion est exécutée par vérification de l'authenticité du serveur SQL).
   - Identifiant du compte pour se connecter au serveur SQL (par exemple, Administrator).
   - Mot de passe du compte pour se connecter au serveur SQL (par exemple, 1234).

Suite à la restauration, les paramètres suivants par défaut de Kaspersky Anti-Virus sont enregistrés dans le stockage de configuration :

- les paramètres au niveau du groupe, si la configuration au niveau du groupe est incorrecte ou absente dans le stockage de configuration ;
- les paramètres au niveau de l'entreprise et au niveau du groupe, si la configuration au niveau de l'entreprise et au niveau du groupe est incorrecte ou absente dans le stockage de configuration.

La configuration de Kaspersky Anti-Virus au niveau du serveur reste inchangée. L'application est opérationnelle sur le serveur.

RESTAURATION DE L'APPLICATION

Si les fichiers de Kaspersky Anti-Virus dans le dossier d'installation sont corrompus ou ont été supprimés par inadvertance, vous pouvez restaurer le fonctionnement de l'application à l'aide de la procédure de restauration.

La procédure de restauration s'effectue dans les fenêtres de l'Assistant d'installation.

Vous pouvez refuser la restauration à n'importe quelle étape de l'Assistant.

Pour restaurer l'application, vous devez fermer la Console d'administration de Kaspersky Anti-Virus.

Pour restaurer Kaspersky Anti-Virus sur le serveur, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant d'installation de l'application à l'aide des outils standard d'installation et de suppression des programmes de Microsoft Windows. Cliquez sur le bouton **Suivant**.
2. Dans la fenêtre **Modification, restauration et suppression des modules**, cliquez sur le bouton **Restaurer**.
3. Dans la fenêtre **Le programme est prêt à restaurer Kaspersky Anti-Virus 8.5 for Microsoft® ISA Server et Forefront® TMG**, cliquez sur le bouton **Restaurer**. L'Assistant d'installation affiche la progression de la restauration de l'application.

   Le processus de restauration requiert le redémarrage du service Microsoft Firewall. L'Assistant d'installation affiche à l'écran une demande d'arrêt du service. Pour confirmer l'arrêt du service, cliquez sur le bouton **OK**.

   Si vous souhaitez refuser d'arrêter le service, cliquez sur le bouton **Annuler**. La restauration de Kaspersky Anti-Virus sera arrêtée.
4. Cliquez sur le bouton **Terminer** pour fermer la fenêtre de l'Assistant d'installation.

   Avant de fermer la fenêtre, l'Assistant d'installation supprime tous les objets temporaires et les données qu'il a créées et exécute le lancement du service Microsoft Firewall qu'il avait arrêté.

La procédure de restauration n'influence pas les paramètres de Kaspersky Anti-Virus enregistrés dans le stockage de configuration de Microsoft ISA Server/Forefront TMG.

SUPPRESSION DE L'APPLICATION

Cette section contient des informations sur la suppression de Kaspersky Anti-Virus d'un serveur ainsi que des instructions sur la suppression de l'application.

DANS CETTE SECTION

A propos de la suppression de Kaspersky Anti-Virus 45

Suppression de l'application du serveur 47

A PROPOS DE LA SUPPRESSION DE KASPERSKY ANTI-VIRUS

La suppression de Kaspersky Anti-Virus s'effectue pour chaque serveur.

Dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise* (cf. section "*Schémas types de déploiement*" à la page 17), vous pouvez supprimer Kaspersky Anti-Virus de tous les serveurs du groupe/de l'entreprise ou uniquement d'un ou de plusieurs serveurs. Une fois Kaspersky Anti-Virus supprimé d'un ou de plusieurs serveurs, le fonctionnement de l'application sur les autres serveurs ne sera pas perturbé.

En cas de déploiement de Kaspersky Anti-Virus sur les serveurs des groupes, il est recommandé d'installer l'application sur chaque serveur du groupe pour assurer la protection antivirus du réseau.

Pendant la suppression de Kaspersky Anti-Virus du serveur, l'Assistant d'installation effectue les opérations suivantes :

- Supprime du serveur sur lequel a lieu la suppression les modules de Kaspersky Anti-Virus et les données qu'il a créées (y compris le dossier de conservation des données de Kaspersky Anti-Virus).
- Supprime de la Base de données de la sauvegarde et des statistiques les enregistrements relatifs aux objets de la Sauvegarde de ce serveur.
- Supprime les notifications des évènements de Kaspersky Anti-Virus enregistrés dans Microsoft ISA Server / Forefront TMG.

  Les notifications enregistrées de Kaspersky Anti-Virus sont supprimées au moment de la suppression de Kaspersky Anti-Virus du serveur actuel uniquement si le schéma de déploiement n'a pas d'autres serveurs sur lesquels l'application est installée.
- Supprime du stockage de configuration de Microsoft ISA Server/Forefront TMG la configuration de Kaspersky Anti-Virus.

  La suppression de la configuration de Kaspersky Anti-Virus du stockage de configuration de Microsoft ISA Server / Forefront TMG dépend du schéma de déploiement de Kaspersky Anti-Virus et de la présente dans le schéma de déploiement de serveurs utilisant les paramètres de chaque niveau.

  - Schéma de déploiement *Serveur autonome* : en cas de suppression de Kaspersky Anti-Virus du serveur actuel, la configuration de Kaspersky Anti-Virus et les notifications enregistrées de Kaspersky Anti-Virus sont supprimées du stockage de configuration.
  - Schéma de déploiement *Groupe autonome* : en cas de suppression de Kaspersky Anti-Virus du serveur actuel, la configuration est supprimée en fonction de la présence dans le groupe d'autres serveurs sur lesquels serait installé Kaspersky Anti-Virus :
    - Si parallèlement au serveur actuel, il existe d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus, seule la configuration au niveau du serveur (pour le serveur actuel) est supprimée du stockage de configuration.
    - Si parallèlement au serveur actuel, il n'y a pas d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus, la configuration de Kaspersky Anti-Virus est entièrement supprimée.
  - Schéma de déploiement *Entreprise* : en cas de suppression de Kaspersky Anti-Virus du serveur actuel, la configuration est supprimée en fonction de la présence dans le groupe/dans l'entreprise d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus :
    - Si, dans le groupe, parallèlement au serveur actuel, il existe d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus, seule la configuration au niveau du serveur (pour le serveur actuel) est supprimée du stockage de configuration.
    - Si, dans le groupe, parallèlement au serveur actuel, il n'y a pas d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus, mais que Kaspersky Anti-Virus est installé sur les serveurs des autres groupes de l'entreprise, seule la configuration au niveau du serveur (pour le serveur actuel) et au niveau du groupe (pour le groupe auquel appartient le serveur actuel) est supprimée du stockage de configuration.
    - Si, dans l'entreprise, parallèlement au serveur actuel, il n'y a pas d'autres serveurs sur lesquels est installé Kaspersky Anti-Virus, la configuration de Kaspersky Anti-Virus est entièrement supprimée du serveur actuel au moment de la suppression de l'application.

SUPPRESSION DE L'APPLICATION DU SERVEUR

La suppression de Kaspersky Anti-Virus s'effectue à l'aide des outils standard d'installation et de suppression des programmes de Microsoft Windows.

Toutes les opérations de suppression de l'application sont effectuées dans les fenêtres de l'Assistant d'installation.

Vous pouvez refuser la suppression à n'importe quelle étape de l'Assistant. En cas de refus de supprimer l'application, l'Assistant d'installation annule toutes les modifications apportées au système et se termine.

En cas d'erreur lors de la suppression, l'écran affiche un message d'erreur mais la suppression n'est pas interrompue.

Pour supprimer l'application, vous devez fermer la Console d'administration de Kaspersky Anti-Virus.

Pour supprimer Kaspersky Anti-Virus du serveur, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant d'installation de l'application à l'aide des outils standard d'installation et de suppression des programmes de Microsoft Windows. Cliquez sur le bouton **Suivant**.

2. Dans la fenêtre **Modification, restauration et suppression des modules**, cliquez sur le bouton **Supprimer**.

3. Dans la fenêtre **Le programme est prêt à supprimer Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG**, cliquez sur le bouton **Supprimer**. L'Assistant d'installation affiche la progression de la suppression de l'application.

   La suppression requiert le redémarrage du service Microsoft Firewall. L'Assistant d'installation affiche à l'écran une demande d'arrêt du service. Pour confirmer l'arrêt du service, cliquez sur le bouton **OK**.

   Si vous souhaitez refuser d'arrêter le service, cliquez sur le bouton **Annuler**. La suppression de Kaspersky Anti-Virus sera arrêtée.

4. Cliquez sur le bouton **Terminer** pour fermer la fenêtre de l'Assistant d'installation.

   Avant de fermer la fenêtre, l'Assistant d'installation supprime tous les objets temporaires et les données qu'il a créées et exécute le lancement du service Microsoft Firewall qu'il avait arrêté.

CONTACTER LE SUPPORT TECHNIQUE

Cette section contient des informations sur les moyens d'obtenir de l'assistance technique et sur les conditions requises pour obtenir l'aide du Support technique.

DANS CETTE SECTION

Modes d'obtention de l'assistance technique 48

Support Technique par téléphone 48

Obtention de l'assistance technique via Mon Espace Personnel 48

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé la solution à votre problème dans la documentation de l'application ou dans l'une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 8), nous vous recommandons de contacter le 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, il est recommandé de prendre connaissance des Conditions d'accès au Support Technique (http://support.kaspersky.com/support/rules).

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- Par téléphone. Cette méthode permet de contacter les experts du Support Technique en français.
- En envoyant une demande depuis Mon Espace Personnel sur le site Web du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

L'assistance technique est fournie uniquement aux utilisateurs qui ont acheté une licence commerciale d'utilisation de l'application. Les utilisateurs ayant obtenu une licence d'essai n'ont pas droit à l'assistance technique.

SUPPORT TECHNIQUE PAR TELEPHONE

En cas de problème urgent, vous pouvez téléphoner aux experts du Support Technique francophone (http://www.kaspersky.com/fr/support-contact).

Avant de vous adresser au Support Technique, veuillez prendre connaissance des règles applicables (http://support.kaspersky.com/support/details). Nos experts pourront ainsi vous venir en aide plus rapidement.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

Mon Espace personnel est la section qui vous est réservée (https://support.kaspersky.com/fr/PersonalCabinet) sur le site du Support Technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/registration) et obtenir ainsi un numéro de client et un mot de passe pour accéder à votre Espace Personnel. Pour cela, vous devez indiquer le fichier clé (pour de plus amples renseignements sur le fichier, cf. le *Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*).

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- Communiquer avec le Support Technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel ;
- Consulter l'historique complet de votre interaction avec le Support Technique ;
- Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.

Formulaire de demande au Support Technique

Vous pouvez envoyer une demande par voie électronique au Support Technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- Type de demande ;
- Nom et numéro de version de l'application ;
- Contenu de la demande ;
- Numéro de client et mot de passe ;
- Adresse électronique.

L'expert du Support Technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

Demande électronique adressée au Laboratoire d'étude des virus

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

Vous pouvez envoyer au Laboratoire d'étude des virus les types de demandes suivantes :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Anti-Virus ne détecte aucune infection.

  Les experts du Laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de détection d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif de l'application* : Kaspersky Anti-Virus considère un fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas.

- *Demande de description d'un programme malveillant* : vous souhaitez obtenir la description d'un virus détecté par Kaspersky Anti-Virus sur la base du nom de ce virus.

Vous pouvez également envoyer une demande au Laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Mon Espace Personnel.

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur peut activer l'application pendant ou après son installation. Pour activer l'application, l'utilisateur doit avoir le code d'activation ou le fichier de licence.

Analyse du trafic

Analyse des objets transmis via les protocoles (par exemple, HTTP, FTP, SMTP, POP3), en temps réel à l'aide des informations de la version actuelle (dernière version) des bases de Kaspersky Anti-Virus.

Analyseur heuristique

Technologie d'identification des menaces dont les informations ne sont pas reprises dans les bases de Kaspersky Lab. L'analyseur heuristique permet d'identifier les objets dont le comportement dans le système est semblable à celui des menaces. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Par exemple, un objet contenant les séquences de commandes propres aux objets malveillants (ouverture d'un fichier, l'écriture dans un fichier) peut être considéré comme potentiellement infecté.

B

Base de donnees de la sauvegarde et des statistiques

La Base de données sur le serveur SQL conçue pour conserver les informations statistiques sur l'utilisation de l'application et les informations sur les objets dangereux dont les copies sont placées dans la sauvegarde par Kaspersky Anti-Virus.

Bases de Kaspersky Anti-Virus

Bases de données qui contiennent la description des menaces pour la sécurité de l'ordinateur et connues par Kaspersky Lab au moment de l'édition des bases. Les enregistrements dans les bases permettent de détecter le code malveillant dans les objets analysés. Les bases sont formées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

Blocage d'un objet

Interdiction d'accès à un objet de la part d'applications tiers. L'objet bloqué ne peut être lu, exécuté, modifié ni supprimé.

C

Cle active

Clé utilisée actuellement pour faire fonctionner l'application.

Cle supplementaire

Clé attestant du droit d'utilisation de l'application mais non utilisée pour le moment.

Copie de sauvegarde

Création d'une copie de sauvegarde d'un fichier avant qu'il ne soit réparé ou supprimé et placé dans la Sauvegarde avec la possibilité de le restaurer ultérieurement, par exemple en vue de l'analyser à l'aide des bases mises à jour.

D

Duree de validite de la licence

La durée de validité de la licence est la période pendant laquelle vous pouvez utiliser les fonctions de l'application et les services supplémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

F

FICHIER CLE

Fichier du type xxxxxxx.key. Le fichier clé est fourni à l'achat de l'application. Le fichier clé est indispensable à l'utilisation de l'application.

L

LICENCE

La licence est un droit d'utilisation de l'application, limité dans le temps, qui est octroyé dans le cadre du Contrat de licence.

LISTE NOIRE DES CLES

Base de données contenant des informations sur les clés bloquées par Kaspersky Lab. Le contenu du fichier et la liste noire sont mis à jour avec les bases.

M

MISE A JOUR

Fonctionnalité de Kaspersky Lab qui permet de maintenir à jour la protection de l'ordinateur. Pendant la mise à jour, l'application copie les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur, les installe et les met en application.

O

OBJET

Corps du message ou simple pièce jointe, par exemple sous forme de fichier exécutable. Cf. également objet-conteneur.

OBJET-CONTENEUR

Objet composé de plusieurs objets, d'archives, message contenant une pièce jointe. Cf. également Objet.

OBJET INFECTE

Objet dont un extrait de code est identique à un extrait de code d'une menace connue. Les experts de Kaspersky Lab déconseillent d'utiliser ces objets.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient un code modifié d'une menace connue ou un code dont le comportement ressemble à celui d'une menace.

R

REPARATION D'OBJETS

Méthode utilisée pour le traitement des objets infectés qui permet de restaurer les données totalement ou partiellement. Certains objets infectés ne peuvent pas être réparés.

S

SAUVEGARDE

Dossier spécial prévu pour conserver les copies de sauvegarde des objets créés avant leur réparation ou leur suppression.

SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab à partir desquels l'application de Kaspersky Lab obtient la mise à jour des bases et des modules de l'application.

STRATEGIE

Une ou plusieurs règles qui définissent les paramètres de la protection antivirus appliquées uniquement pour les connexions et les protocoles sélectionnés.

L'application prévoit trois types de stratégie : Stratégie de traitement des protocoles, Stratégie d'exclusion de l'analyse et Stratégie d'analyse antivirus.

STRATEGIE D'ANALYSE ANTIVIRUS

Définit les paramètres de détection des menaces et des actions à exécuter sur les objets détectés.

STRATEGIE D'EXCLUSION DE L'ANALYSE

Définit les paramètres d'exclusion des objets de l'analyse antivirus.

STRATEGIE DE TRAITEMENT DES PROTOCOLES

Définit les paramètres de traitement du trafic au niveau des protocoles FTP et HTTP.

SUPPRESSION DE L'OBJET

Méthode de traitement de l'objet qui supprime physiquement l'objet de l'endroit où il a été détecté par l'application (disque dur, dossier, ressource réseau). Il est recommandé d'appliquer cette méthode de traitement aux objets dangereux qui ne peuvent pas être réparés pour telle ou telle raison.

KASPERSKY LAB ZAO

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

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

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

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

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

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'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 trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

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

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

Site officiel de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie de virus :	http://www.securelist.com/fr/
Laboratoire Anti-Virus :	newvirus@kaspersky.com (uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les demandes auprès des experts en virus)
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.

Forefront, Microsoft, SQL Server, Windows, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

INDEX

A

Activation de l'application 32, 38
Architecture de l'application 13
Assistant d'installation 25

B

Base de données de la sauvegarde et des statistiques 13, 25
    paramètres de connexion 29

C

Configuration initiale de l'application 31
Console d'administration 13
    connexion 35

F

Filtre de Kaspersky Anti-Virus 13

H

HTTPS 10

I

Installation complète 26
Installation de la Console d'administration 33

K

Kaspersky Lab ZAO 53

N

Niveau de configuration 14

R

Restauration de la configuration 40
Restauration de l'application 45

S

Schémas de déploiement 17
    Entreprise 17, 20
    Groupe autonome 17, 18
    Serveur autonome 17
Serveur de sécurité 13
Suppression de l'application 45

T

Type d'installation 25