KASPERSKY LAB

Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition

MANUEL DE L'ADMINISTRATEUR

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ENTERPRISE EDITION

Manuel de l'administrateur

Tél., fax : +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
http://www.kaspersky.com/fr

Date d'édition : lundi 28 juillet 2008

Sommaire

CHAPITRE 1. INTRODUCTION 14
1.1. Informations générales sur Kaspersky Anti-Virus 14
1.1.1. Protection en temps réel et analyse à la demande 15
1.1.2. Présentation des menaces identifiées par Kaspersky Anti-Virus 16
1.1.3. Présentation des objets infectés, suspects et potentiellement dangereux 20
1.2. Informations relatives à Kaspersky Anti-Virus 21
1.2.1. Sources d'informations pour une recherche indépendante 22
1.2.2. Contacter le service ventes 24
1.2.3. Contacter le service d'assistance technique 24
1.2.4. Discussion sur les applications de Kaspersky Lab dans le forum 26

CHAPITRE 2. UTILISATION DE LA CONSOLE DE KASPERSKY ANTI-VIRUS DANS MMC ET ACCES AUX SES FONCTIONS 28
2.1. Présentation de la console de Kaspersky Anti-Virus dans MMC 28
2.2. Configuration avancée après l'installation de la console de Kaspersky Anti-Virus dans MMC sur un autre ordinateur 29
2.2.1. Ajout d'utilisateurs de Kaspersky Anti-Virus au groupe KAVWSEE Administrators sur le serveur protégé 30
2.2.2. Autorisation des connexions de réseau sous un serveur tournant sous Microsoft Windows Server 2008 pour le service d'administration de Kaspersky Anti-Virus 31
2.2.3. Autorisation des connexions de réseau pour la console de Kaspersky Anti-Virus dans MMC sous Microsoft Windows XP avec Service Pack 1 . 32
2.2.4. Autorisation des connexions de réseau pour la console de Kaspersky Anti-Virus dans MMC sous Microsoft Windows XP avec Service Pack 2 ou Microsoft Windows Vista 33
2.3. Lancement de la console de Kaspersky Anti-Virus depuis le menu *Démarrer* 35
2.4. Icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches 36
2.5. Fenêtre de la console de Kaspersky Anti-Virus 38
2.6. Restriction des privilèges d'accès aux fonctions de Kaspersky Anti-Virus 38

2.6.1. Présentation des privilèges d'accès aux fonctions de Kaspersky Anti-Virus 39
2.6.2. Configuration des privilèges d'accès aux fonctions de Kaspersky Anti-Virus 41
2.7. Lancement et arrêt du service de Kaspersky Anti-Virus 44

CHAPITRE 3. PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS 45
3.1. Présentation des paramètres généraux de Kaspersky Anti-Virus 45
3.2. Configuration des paramètres généraux de Kaspersky Anti-Virus 46

CHAPITRE 4. IMPORTATION ET EXPORTATION DES PARAMETRES DE KASPERSKY ANTI-VIRUS 50
4.1. Présentation de l'importation et de l'exportation des paramètres 50
4.2. Exportation des paramètres 51
4.3. Importations des paramètres 52

CHAPITRE 5. ADMINISTRATION DES TACHES 54
5.1. Catégories de tâches dans Kaspersky Anti-Virus 54
5.2. Nouvelle tâche 56
5.3. Enregistrement d'une tâche après modification de ses paramètres 58
5.4. Renommer 59
5.5. Suppression d'une tâche 59
5.6. Lancement / suspension / rétablissement / arrêt manuel d'une tâche 60
5.7. Programmation des tâches 60
5.7.1. Programmation d'une tâche 60
5.7.2. Activation et désactivation de l'exécution programmée 64
5.8. Consultation des statistiques des tâches 64
5.9. Utilisation des comptes utilisateur pour l'exécution des tâches 65
5.9.1. Présentation de l'utilisation des comptes utilisateur pour l'exécution des tâches 65
5.9.2. Définition du compte utilisateur pour l'exécution de la tâche 66

CHAPITRE 6. PROTECTION EN TEMPS REEL DES FICHIERS 68
6.1. Présentation des tâches de la protection en temps réel 68
6.2. Configuration de la tâche *Protection en temps réel des fichiers* 69
6.2.1. Couverture de protection dans la tâche *Protection en temps réel des fichiers* 72
6.2.1.1. Présentation de la constitution d'une couverture de protection dans la tâche *Protection en temps réel des fichiers* 72

6.2.1.2. Couvertures de protection prédéfinies ... 73
6.2.1.3. Constitution de la couverture de protection ... 75
6.2.1.4. Couverture de protection virtuelle ... 76
6.2.1.5. Création d'une couverture de protection virtuelle : inclusion des disques, répertoires et fichiers dynamiques dans la couverture de protection ... 77
6.2.2. Configuration des paramètres de sécurité du noeud sélectionné ... 79
6.2.2.1. Sélection des niveaux prédéfinis de protection dans la tâche *Protection en temps réel des fichiers* ... 79
6.2.2.2. Configuration manuelle des paramètres de sécurité ... 82
6.2.2.3. Utilisation de modèles dans la tâche *Protection en temps réel des fichiers* ... 86
6.2.3. Sélection du mode de protection des objets ... 90
6.3. Statistiques de la tâche *Protection en temps réel des fichiers* ... 92
6.4. Configuration de la tâche *Analyse des scripts* ... 94
6.5. Statistiques de la tâche *Analyse des scripts* ... 95

CHAPITRE 7. INTERDICTION DE L'ACCES DES ORDINATEURS DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS ... 97
7.1. Interdiction de l'accès des ordinateurs au serveur protégé ... 97
7.2. Activation ou désactivation de l'interdiction automatique d'accès des ordinateurs ... 98
7.3. Configuration des paramètres d'interdiction automatique de l'accès des ordinateurs ... 99
7.4. Exclusion d'ordinateurs de l'interdiction automatique (ordinateurs de confiance) ... 101
7.5. Prévention des épidémies virales ... 102
7.6. Consultation de la liste des ordinateurs dont l'accès au serveur est interdit ... 104
7.7. Interdiction manuelle de l'accès des ordinateurs ... 105
7.8. Levée de l'interdiction de l'accès des ordinateurs ... 107
7.9. Consultation des statistiques de l'interdiction ... 107

CHAPITRE 8. ZONE DE CONFIANCE ... 109
8.1. Présentation de la zone de confiance de Kaspersky Anti-Virus ... 109
8.2. Ajout d'exclusions à la zone de confiance ... 111
8.2.1. Ajout de processus à la liste des processus de confiance ... 111
8.2.2. Désactivation de la protection en temps réel des fichiers durant la copie de sauvegarde ... 115
8.2.3. Ajout de règles d'exclusion ... 116

8.3. Application de la zone de confiance 120

CHAPITRE 9. ANALYSE A LA DEMANDE 121
9.1. Présentation des tâches d'analyse à la demande 121
9.2. Configuration des tâches d'analyse à la demande 122
9.2.1. Couverture de l'analyse dans les tâches d'analyse à la demande 124
9.2.1.1. Présentation de la constitution d'une couverture d'analyse dans les tâches d'analyse à la demande 125
9.2.1.2. Couvertures d'analyse prédéfinies 125
9.2.1.3. Constitution de la couverture d'analyse 127
9.2.1.4. Inclusion des disques de réseau , des répertoires ou des fichiers dans la couverture d'analyse 129
9.2.1.5. Création d'une couverture d'analyse virtuelle : inclusion des disques, répertoires et fichiers dynamiques dans la couverture d'analyse 129
9.2.2. Configuration des paramètres de sécurité pour le noeud sélectionné 132
9.2.2.1. Sélection du niveau de sécurité prédéfini dans les tâches d'analyse à la demande 132
9.2.2.2. Configuration manuelle des paramètres de sécurité 136
9.2.2.3. Utilisation des modèles dans les tâches d'analyse à la demande 140
9.3. Exécution en arrière-plan de la tâche d'analyse à la demande 145
9.4. Statistiques des tâches d'analyse à la demande 147

CHAPITRE 10. MISE A JOUR DES BASE ET DES MODULES LOGICIELS DE KASPERSKY ANTI-VIRUS 151
10.1. Présentation de la mise à jour des bases de Kaspersky Anti-Virus 152
10.2. Présentation de la mise à jour des modules de Kaspersky Anti-Virus 153
10.3. Schémas de mise à jour des bases et des modules logiciels des applications antivirus dans l'entreprise 154
10.4. Tâches de mise à jour 158
10.5. Configuration des tâches liées à la mise à jour 160
10.5.1. Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour et paramètres régionaux 160
10.5.2. Configuration des paramètres de la tâche *Mise à jour des modules de l'application* 165
10.5.3. Configuration des paramètres de la tâche *Copie des mises à jour* 167
10.6. Statistiques des tâches de mise à jour 169
10.7. Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus 170

10.8. Remise à l'état antérieur à la mise à jour des modules logiciels 170

CHAPITRE 11. ISOLEMENT DES OBJETS SUSPECTS. UTILISATION DE LA QUARANTAINE..... 171
11.1. Présentation de l'isolement des objets suspects 171
11.2. Consultation des objets en quarantaine 172
11.2.1. Tri des objets en quarantaine 175
11.2.2. Filtrage des objets en quarantaine..... 175
11.3. Analyse des objets en quarantaine. Paramètres de la tâche *Analyse des objets en quarantaine*..... 177
11.4. Restauration des objets de la quarantaine 179
11.5. Mise en quarantaine des fichiers..... 183
11.6. Suppression des objets de la quarantaine 184
11.7. Envoi des objets suspects à Kaspersky Lab pour examen 184
11.8. Configuration de la quarantaine 186
11.9. Statistiques de quarantaine..... 188

CHAPITRE 12. SAUVEGARDE DES OBJETS AVANT LA REPARATION / LA SUPPRESSION. UTILISATION DE LA SAUVEGARDE 190
12.1. Présentation de la sauvegarde des objets avant la réparation / la suppression 190
12.2. Consultation des fichiers du dossier de sauvegarde 191
12.2.1. Tri des fichiers de la sauvegarde..... 194
12.2.2. Filtrage des fichiers de la sauvegarde 194
12.3. Restauration des fichiers depuis la sauvegarde..... 196
12.4. Suppression des fichiers depuis la sauvegarde 200
12.5. Configuration des paramètres de la sauvegarde..... 200
12.6. Statistiques de sauvegarde..... 202

CHAPITRE 13. CONSIGNATION DES EVENEMENTS..... 204
13.1. Moyens d'enregistrement des événements..... 204
13.2. Rapports sur l'exécution des tâches..... 205
13.2.1. Présentation des rapports sur l'exécution des tâches 205
13.2.2. Consultation des rapports de synthèse. Etat des rapports de synthèse 206
13.2.3. Tri des rapports..... 210
13.2.4. Consultation du rapport détaillé sur l'exécution de la tâche..... 211
13.2.5. Exportation des informations du rapport détaillé dans un fichier texte... 216
13.2.6. Suppression des rapports 216

13.2.7. Configuration du niveau de détail des informations dans les rapports et le journal des événements 217
13.3. Journal d'audit système 219
13.3.1. Tri des événements dans le journal d'audit système 221
13.3.2. Filtrage des événements dans le journal d'audit système 222
13.3.3. Suppression des événements du journal d'audit système 223
13.4. Statistiques de Kaspersky Anti-Virus 224
13.5. Journal des événements de Kaspersky Anti-Virus dans la console « Event Viewer » 228

CHAPITRE 14. INSTALLATION ET SUPPRESSION DES CLES 230
14.1. Présentation des clés de Kaspersky Anti-Virus 230
14.2. Consultation des informations relatives aux clés installées 232
14.3. Installation de la clé 233
14.4. Suppression de la clé 235

CHAPITRE 15. CONFIGURATION DES NOTIFICATIONS 236
15.1. Moyens de notification de l'administrateur et des utilisateurs 236
15.2. Configuration des notifications 238

CHAPITRE 16. ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA LA LIGNE DE COMMANDE 247
16.1. Affichage de l'aide sur les commandes de Kaspersky Anti-Virus. KAVSHELL HELP 249
16.2. Lancement et arrêt du service de Kaspersky Anti-Virus. KAVSHELL START, KAVSHELL STOP 249
16.3. Analyse du secteur indiqué. KAVSHELL SCAN 250
16.4. Lancement de la tâche *Analyse complète de l'ordinateur.* KAVSHELL FULLSCAN 255
16.5. Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK 256
16.6. Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP 258
16.7. Lancement de la tâche de mise à jour des bases de Kaspersky Anti-Virus. KAVSHELL UPDATE 258
16.8. Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus. KAVSHELL ROLLBACK 264
16.9. Installation et suppression des clés. KAVSHELL LICENSE 264
16.10. Activation, configuration et désactivation de la constitution d'un journal de traçage. KAVSHELL TRACE 265

16.11. Activation et désactivation de la création de fichiers de vidage. KAVSHELL DUMP 267
16.12. Importations des paramètres. KAVSHELL IMPORT 268
16.13. Exportation des paramètres. KAVSHELL EXPORT 269

CHAPITRE 17. CODE DE RETOUR 270

CHAPITRE 18. ADMINISTRATION DE KASPERSKY ANTI-VIRUS ET CONSULTATION DE SON ETAT 277
18.1. Lancement et arrêt du service de Kaspersky Anti-Virus 277
18.2. Consultation de l'état de la protection du serveur 278
18.3. Consultation des statistiques de Kaspersky Anti-Virus 281
18.4. Consultation des informations relatives à Kaspersky Anti-Virus 283
18.5. Consultation des informations relatives aux clés installées 284

CHAPITRE 19. CREATION ET CONFIGURATION DE STRATEGIE 287
19.1. Présentation des stratégies 287
19.2. Création d'une stratégie 288
19.3. Configuration des stratégies 294
19.4. Désactivation / rétablissement du lancement programmé des tâches prédéfinies locales 299

CHAPITRE 20. CONFIGURATION DE KASPERSKY ANTI-VIRUS DANS LA BOITE DE DIALOGUE PARAMETRES DE L'APPLICATION 301
20.1. Boîte de dialogue *Paramètres de l'application* 301
20.2. Configuration des paramètres généraux de Kaspersky Anti-Virus 303
20.3. Interdiction de l'accès des ordinateurs 307
20.3.1. Activation ou désactivation de l'interdiction automatique d'accès des ordinateurs 308
20.3.2. Configuration des paramètres d'interdiction automatique de l'accès des ordinateurs 309
20.3.3. Exclusion d'ordinateurs de l'interdiction (ordinateurs de confiance) 311
20.3.4. Prévention des épidémies virales 312
20.3.5. Consultation de la liste des accès interdits au serveur 313
20.3.6. Interdiction manuelle de l'accès des ordinateurs 315
20.3.7. Levée de l'interdiction de l'accès des ordinateurs 316
20.4. Administration des objets en quarantaine et configuration de la quarantaine 317
20.4.1. Fonctions de quarantaine et leur configuration 317

20.4.2. Configuration de la quarantaine ... 318
20.5. Administration des fichiers de la sauvegarde et configuration de celle-ci ... 320
20.5.1. Fonctions de la sauvegarde et moyens de configuration ... 320
20.5.2. Configuration des paramètres de la sauvegarde ... 321
20.6. Configuration des notifications ... 322
20.6.1. Informations générales ... 322
20.6.2. Configuration des notifications adressées à l'administrateur et aux utilisateurs sur l'onglet *Notification* ... 324
20.7. Administration de la zone de confiance ... 325
20.7.1. Ajout de processus à la liste des processus de confiance ... 325
20.7.2. Désactivation de la protection en temps réel des fichiers durant la copie de sauvegarde ... 327
20.7.3. Ajout d'exclusions à la zone de confiance ... 329
20.7.4. Application de la zone de confiance ... 332

CHAPITRE 21. CREATION ET CONFIGURATION DE TACHES ... 334
21.1. Présentation de la création des tâches ... 334
21.2. Création d'une tâche ... 335
21.3. Configuration de la tâche ... 345
21.4. Administration de l'analyse complète des serveurs Octroi du statut *Tâche d'analyse complète de l'ordinateur* à la tâche d'analyse à la demande ... 347

CHAPITRE 22. COMPTEUR DE PERFORMANCE POUR L'APPLICATION « SYSTEM MONITOR » ... 350
22.1. Présentation des compteurs de performances de Kaspersky Anti-Virus ... 350
22.2. Total de requêtes rejetées ... 351
22.3. Total de requêtes ignorées ... 352
22.4. Nombre de requêtes non traitées en raison d'un manque de ressources système ... 353
22.5. Nombre de requêtes envoyées pour traitement ... 354
22.6. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers ... 355
22.7. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers ... 356
22.8. Nombre d'objets infectés dans la file de traitement ... 356
22.9. Nombre d'objets traités par seconde ... 358

CHAPITRE 23. COMPTEURS ET PIEGES SNMP DE KASPERSKY ANTI-VIRUS ... 360
23.1. Présentation des compteurs et pièges SNMP de Kaspersky Anti-Virus ... 360
23.2. Compteurs SNMP de Kaspersky Anti-Virus ... 360

23.2.1. Compteurs de performances ... 361
23.2.2. Compteurs généraux ... 361
23.2.3. Compteur de mise à jour ... 362
23.2.4. Compteurs de protection en temps réel ... 362
23.2.5. Compteurs de quarantaine ... 364
23.2.6. Compteurs de sauvegarde ... 364
23.2.7. Compteurs d'interdiction d'accès des ordinateurs au serveur ... 364
23.2.8. Compteurs d'analyse des scripts ... 365
23.3. Pièges SNMP ... 365

ANNEXE A. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE ... 374

ANNEXE B. DESCRIPTION DES PARAMETRES GENERAUX DE KASPERSK ANTI-VIRUS, DES PARAMETRES DE SES FONCTIONS ET DE SES TACHES ... 376
B.1. Paramètres généraux de Kaspersky Anti-Virus ... 376
B.1.1. Nombre maximum de processus de travail actifs ... 377
B.1.2. Nombre de processus pour la protection en temps réel ... 378
B.1.3. Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan ... 379
B.1.4. Restauration des tâches ... 380
B.1.5. Durée de conservation des rapports ... 381
B.1.6. Durée de conservation des événements dans le journal d'audit système ... 382
B.1.7. Actions dans le fonctionnement sur la source d'alimentation de secours ... 383
B.1.8. Seuil de déclenchement des événements ... 383
B.1.9. Paramètres du journal de traçage ... 384
B.1.9.1. Constitution d'un journal de traçage ... 385
B.1.9.2. Dossier contenant les fichiers du journal de traçage ... 386
B.1.9.3. Niveau de détail du journal de traçage ... 387
B.1.9.4. Taille d'un fichier du journal de traçage ... 387
B.1.9.5. Traçage de sous-systèmes individuels de Kaspersky Anti-Virus ... 388
B.1.10. Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus ... 390
B.2. Paramètres de planification des tâches ... 391
B.2.1. Fréquence ... 392
B.2.2. Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche ... 393
B.2.3. Date de la fin de validité de la planification ... 394

B.2.4. Durée maximale de l'exécution d'une tâche ... 395
B.2.5. Intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue ... 396
B.2.6. Lancement des tâches non exécutées ... 396
B.2.7. Répartition des lancements dans l'intervalle, min ... 397
B.3. Paramètres de protection dans la tâche *Protection en temps réel des fichiers* et dans les tâches d'analyse à la demande ... 398
B.3.1. Mode de protection ... 399
B.3.2. Objets à analyser ... 400
B.3.3. Analyse uniquement des objets neufs et modifiés ... 402
B.3.4. Traiter les objets composés ... 402
B.3.5. Actions à exécuter sur les objets infectés ... 404
B.3.5.1. Dans la tâche *Protection en temps réel des fichiers* ... 404
B.3.5.2. Dans les tâches d'analyse à la demande ... 405
B.3.6. Actions à exécuter sur les objets suspects ... 406
B.3.6.1. Dans la tâche *Protection en temps réel des fichiers* ... 406
B.3.6.2. Dans les tâches d'analyse à la demande ... 407
B.3.7. Actions en fonction du type de menace ... 408
B.3.8. Exclusion des objets ... 410
B.3.9. Exclusion des menaces ... 411
B.3.10. Durée maximale de l'analyse d'un objet ... 413
B.3.11. Taille maximale de l'objet composé à analyser ... 413
B.3.12. Application de la technologie iChecker ... 414
B.3.13. Application de la technologie iSwift ... 415
B.4. Paramètres d'interdiction automatique de l'accès des ordinateurs au serveur ... 416
B.4.1. Activation / désactivation de l'interdiction de l'accès des ordinateurs au serveur ... 417
B.4.2. Actions à exécuter sur les ordinateurs infectés ... 417
B.4.3. Liste des ordinateurs de confiance ... 419
B.4.4. Prévention des épidémies virales ... 419
B.5. Paramètres des tâches de mise à jour ... 422
B.5.1. Source des mises à jour ... 423
B.5.2. Mode du serveur FTP pour la connexion au serveur protégé ... 424
B.5.3. Délai d'attente lors de la connexion à la source des mises à jour ... 425
B.5.4. Utilisation et paramètres du serveur proxy ... 425

B.5.4.1. Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour ... 426
B.5.4.2. Paramètres du serveur proxy ... 427
B.5.4.3. Méthode de vérification de l'authenticité lors de l'accès au serveur proxy ... 428
B.5.5. Paramètres régionaux pour l'optimalisation de la réception des mises à jour (Emplacement) ... 429
B.5.6. Paramètres de la tâche de *Mise à jour des modules de l'application* ... 430
B.5.6.1. Copie et installation des mises à jour critiques ou simple vérification de leur présence ... 431
B.5.6.2. Obtention d'informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus ... 431
B.5.7. Paramètres de la tâche *Copie des mises à jour* ... 432
B.5.7.1. Composition des mises à jour ... 432
B.5.7.2. Dossier pour l'enregistrement des mises à jour ... 434
B.6. Paramètres de quarantaine ... 434
B.6.1. Répertoire de quarantaine ... 435
B.6.2. Taille maximale de la quarantaine ... 436
B.6.3. Seuil d'espace libre dans la quarantaine ... 436
B.6.4. Restaurer dans le dossier ... 437
B.7. Paramètres de sauvegarde ... 438
B.7.1. Dossier de sauvegarde ... 438
B.7.2. Taille max. du dossier de sauvegarde ... 439
B.7.3. Seuil d'espace libre de la sauvegarde ... 440
B.7.4. Restaurer dans le dossier ... 441

ANNEXE C. KASPERSKY LAB ... 443
C.1. Autres produits antivirus ... 444
C.2. Coordonnées ... 456

INDEX ... 457

ANNEXE D. CONTRAT DE LICENCE ... 463

CHAPITRE 1. INTRODUCTION

Ce guide décrit l'utilisation de l'application **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** (par la suite, Kaspersky Anti-Virus).

Le point 1.1 à la page 14 contient des informations générales sur Kaspersky Anti-Virus, une description de ses fonctions de protection et des menaces identifiées.

La Partie 1 de ce manuel, intitulée*Configuration et administration via la console MMC* décrit l'administration de Kaspersky Anti-Virus via la console installée sur le serveur protégé ou sur le poste de travail distant.

Pour savoir comment administrer Kaspersky Anti-Virus via la ligne de commande du serveur protégé, lisez la Partie 2, *Administration de Kaspersky Anti-Virus via la ligne de commande*.

La Partie 3, *Configuration et administration via Kaspersky Administration Kit* décrit l'administration centralisée de la protection des serveurs dotés de Kaspersky Anti-Virus à l'aide de Kaspersky Administration Kit.

La Partie 4, *Compteurs de Kaspersky Anti-Virus* décrit les compteurs de Kaspersky Anti-Virus pour l'application « Moniteur système » ainsi que les compteurs et les pièges SNMP.

Si vous n'avez pas trouvé la réponse à vos questions dans ce document, vous pouvez consulter d'autres sources d'informations sur Kaspersky Anti-Virus(cf. point 1.2, p. 21).

1.1. Informations générales sur Kaspersky Anti-Virus

Kaspersky Anti-Virus protège les serveurs sous Microsoft Windows contre les menaces qui accompagnent l'échange de fichiers. L'utilisation de Kaspersky Anti-Virus est prévue dans les réseaux Intranet des moyennes ou grandes entreprises. Les utilisateurs de Kaspersky Anti-Virus sont les administrateurs du réseau et les personnes chargées de la protection du réseau contre les virus.

Kaspersky Anti-Virus peut être installé sur des serveurs exécutant diverses fonctions : serveurs de terminaux et serveurs d'impression, serveurs d'applications et contrôleurs de domaines ainsi que sur les serveurs de fichiers ; ils sont les plus exposés aux infections car ils échangent les fichiers avec les postes de travail des utilisateurs.

La protection du serveur sur lequel Kaspersky Anti-Virus est installé peut être administrée de diverses manières : à l'aide de la console de Kaspersky Anti-Virus dans MMC, à l'aide de la ligne de commande et même à l'aide de Kaspersky Administration Kit pour l'administration centralisée de la protection de plusieurs serveurs dotés chacun de Kaspersky Anti-Virus Il est possible de consulter les compteurs de performance de Kaspersky Anti-Virus pour l'application « Moniteur système **»** ainsi que les compteurs et les pièges SNMP.

Ce chapitre aborde les sujets suivants :

- Les fonctions *Protection en temps réel* et *Analyse à la demande* de Kaspersky Anti-Virus (cf. point 1.1.1, p. 15) ;
- Les types de menaces identifiées et neutralisées par Kaspersky Anti-Virus (cf. point 1.1.2 , p. 16) ;
- La méthode utilisée par Kaspersky Anti-Virus pour découvrir les objets infectés, suspects ou présentant un risque potentiel (cf. point 1.1.3, p. 20).

1.1.1. Protection en temps réel et analyse à la demande

Vous pouvez protéger les serveurs à l'aide de deux fonctions de Kaspersky Anti-Virus : la *Protection en temps réel* et l'*Analyse à la demande*. Ces fonctions peuvent être activées ou désactivées manuellement ou selon un programme défini.

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

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

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

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

Kaspersky Anti-Virus ne recherche pas seulement les virus dans les objets. Il s'intéresse également aux autres types de menaces comme les chevaux de Troie, les logiciels publicitaires ou les logiciels espion. Pour en savoir plus sur les menaces identifiées et neutralisées par Kaspersky Anti-Virus, lisez le point 1.1.2 à la page 16.

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

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

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

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

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

1.1.2. Présentation des menaces identifiées par Kaspersky Anti-Virus

Kaspersky Anti-Virus est capable d'identifier des centaines de milliers de programmes malveillants différents dans les objets du système de fichiers. Certains de ces programmes présentent un risque élevé pour l'utilisateur tandis que d'autres sont uniquement dangereux dans certaines conditions. Lorsqu'il découvre un programme malveillant dans un objet, Kaspersky Anti-Virus le place dans une catégorie définie avec un niveau de danger propre (élevé, moyen ou faible).

Kaspersky Anti-Virus prévoit les catégories de programmes malveillants suivantes :

- Les virus et les vers (Virware) ;
- Les chevaux de Troie (Trojware) ;
- Les autres programmes malveillants (Malware) ;
- Les programmes au contenu pornographique (Pornware) ;

- Les logiciels publicitaires (Adware) ;
- Les applications présentant un risque potentiel (Riskwares).

Remarque

Vous pouvez consulter le niveau de danger d'une menace présente dans les objets suspects identifiés dans le noeud **Quarantaine** (Chapitre 11, p. 171) ; le niveau de danger des menaces dans les objets infectés figure dans le noeud **Sauvegarde** (Chapitre 12, p. 190).

Vous trouvrez ci-après une brève description des menaces. Pour en savoir plus sur les programmes malveillants et leur classification, vous pouvez consultez le site de l'Encyclopédie des virus de Kaspersky Lab (http://www.viruslist.com/fr/viruses/encyclopedia).

Les virus et les vers (Virware)

Niveau de danger : élevé

Cette catégorie reprend les virus classiques et les vers de réseau.

Un virus classique (catégorie Virus) infecte les fichiers d'autres programmes ou les données. Il y ajoute son code afin de pouvoir prendre les commandes à l'ouverture du programme. Une fois qu'un virus traditionnel a pénétré dans le système, il s'active suite à un événement quelconque puis réalise son action malveillante.

Les virus traditionnels se distinguent par leur environnement et leur moyen d'infection.

Par *environnement*, il faut entendre les zones de l'ordinateur, du système d'exploitation ou des applications où s'infiltre le code du virus. En fonction de l'environnement, nous distinguons les virus de fichier, les virus de démarrage, les virus de macro et les virus de script.

L'expression *moyen d'infection* désigne les différentes méthodes utilisées pour introduire le code du virus dans les objets qui sont infectés. Il existe une multitude de types de virus différents en fonction du moyen d'infection. Les virus *qui écrasent* (overwriting) remplace le code du fichier infecté par leur propre code et élimine ainsi son contenu. Le fichier infecté ne fonctionne plus et il ne peut être restauré. Les virus *parasites* (parasitic) changent le code des fichiers. Ceux ci demeurent complètement ou partiellement opérationnels. *Les virus compagnons* (Companion) ne modifient pas les fichiers mais créent des doubles. Au lancement du fichier infecté, l'administration revient au double, à savoir le virus. Il existe également les *virus liens* (link), qui *infectent les modules objet* (OBJ), *les virus* qui *infectent les bibliothèques des compilateurs* (LIB), *les virus* qui *infectent les textes source du programmes* et d'autres.

Le code **du ver de réseau** (catégorie Worm), à l'instar du code du virus classique, s'active après avoir infecté l'ordinateur puis, il exécute son action malveillante. Le ver de réseau doit son nom à sa capacité de « ramper » d'un ordinateur à l'autre ; il diffuse ses copies via divers moyens de communication.

Le mode de propagation est le seul élément qui permet de différencier les vers de réseau. Il peut s'agir de *vers de messagerie qui utilisent les clients de messagerie Internet*, *de vers dans les canaux IRC*, *de vers dans les réseaux d'échange de fichiers* et d'autres *vers de réseau*. Parmi les autres vers de réseau, citons les vers qui diffusent leur copie dans les ressources de réseau, qui s'infiltrent dans les systèmes d'exploitation via leurs vulnérabilités ou celles des applications installées, qui entrent dans les ressources de réseau publiques ou qui sont associés à d'autre menaces.

La majorité des vers de réseau peut se propager très rapidement.

Les vers de réseau nuisent non seulement à l'ordinateur infecté, mais jettent également le discrédit sur le propriétaire de cet ordinateur, entraînent un paiement complémentaire pour le trafic de réseau généré et polluent les canaux Internet.

Chevaux de Troie (Trojware)

Niveau de danger : élevé

Les chevaux de Troie (catégories Trojan, Backdoor, Rootkit et autres) réalisent sur l'ordinateur des actions qui ne sont pas autorisées par l'utilisateur telles que le vol de mots de passe, la consultation de ressources Internet ou le téléchargement et l'installation d'autres programmes.

A la différence des virus traditionnels, les chevaux de Troie ne se propagent pas automatiquement en pénétrant dans des fichiers et en les infectant. Ils répondent aux commandes d'un « maître ». Ceci étant dit, les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnels.

Les chevaux de Troie les plus dangereux sont les *chevaux de Troie d'administration à distance* (Backdoor). Lorsqu'ils sont exécutés, ces programmes s'installent dans le système à l'insu de l'utilisateur et réalisent une administration cachée : ils suppriment des données sur le disque, entraînent le gel du système ou envoient des informations à leurs auteurs.

Les outils de dissimulation d'activité (Rootkit) se distinguent parmi les chevaux de Troie. A l'instar des autres chevaux de Troie, les outils de dissimulation d'activité pénètrent dans le système à l'insu de l'utilisateur. Ils n'exécutent pas d'actions malveillantes mais dissimulent d'autres programmes malveillants et leurs activité, ce qui prolonge la présence de ces programmes dans le système infecté. Les outils de dissimulation d'activité peuvent dissimuler des fichiers, des processus dans la mémoire de l'ordinateur infecté ou des clés de registre lancées

par les programmes malveillants. Les outils de dissimulation d'activité peuvent dissimuler les requêtes adressées par les individus mal intentionnés au système.

Les autres programmes malveillants (Malware)

Niveau de danger : moyen

Les autres programmes malveillants ne présentent pas une menace pour l'ordinateur sur lequel ils sont exécutés mais ils peuvent intervenir dans l'organisation d'attaques de réseau sur des serveurs distants, dans l'intrusion dans d'autres ordinateurs ou dans la création d'autres virus ou chevaux de Troie.

Les autres programmes malveillants présentent diverses facettes. *Les attaques de réseau* (catégorie DoS (Denial of Service) envoient une multitude de requêtes vers des serveurs distants, ce qui les met hors ligne. *Les mauvaises blagues* (types BadJoke, Hoax) effraient les utilisateurs à l'aide de messages semblables à des virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque dur qui, en fin de compte, n'aura pas lieu. *Les crypteurs* (catégorie FileCryptor, PolyCryptor) chiffrent d'autres programmes malveillants afin de dissimuler leur présence contre l'analyse antivirus. *Les constructeurs* (catégorie Constructor) permettent de produire le code source des virus, des modules objets ou des fichiers infectés. *Les utilitaires de courrier indésirable* (catégorie SpamTool) collectent des adresses de messagerie sur l'ordinateur infecté ou le transforment en machine de diffusion de messages non sollicités.

Programmes au contenu pornographique (Pornware)

Niveau de danger : moyen

Les programmes au contenu pornographique appartiennent à la catégorie des programmes potentiellement dangereux (not-a-virus). Ils possèdent des fonctions qui peuvent nuire à l'utilisateur uniquement lorsque certaines conditions sont remplies.

Ces programmes sont liés à l'affichage d'informations à caractère pornographique. Ces programmes peuvent être répartis en trois groupes en fonction de leur comportement : *les numéroteurs* (Porn-Dialer), *les programmes de chargement de fichiers depuis Internet* (Porn-Downloader) et *les instruments* (Porn-Tool). Les numéroteurs établissent une connexion via le modem avec des sites Internet pornographiques payants tandis que les programmes de téléchargement téléchargent du contenu pornographique sur l'ordinateur. Les instruments regroupent les programmes liés à la recherche et à l'affichage de contenu pornographique (par exemple, des barres d'outils spéciales pour les navigateurs ou des lecteurs vidéo particuliers).

Les logiciels publicitaires (Adware)

Niveau de danger : moyen

Les logiciels publicitaires présentent uniquement un danger potentiel (catégorie not-a-virus). Ils sont intégrés à d'autres programmes pour afficher des messages

publicitaires dans l'interface du programme hôte. Bon nombre d'entre eux ne se contentent pas d'afficher des publicités dans l'interface ; ils recueillent également des données personnelles sur l'utilisateur qu'ils transmettent à leur auteur, ils modifient divers paramètres du navigateur (page d'accueil et recherche, niveau de sécurité, etc.) et ils créent un trafic sur lequel l'utilisateur n'a aucun contrôle. Les actions des logiciels publicitaires peuvent non seulement provoquer une violation de la politique de sécurité mais également entraîner des pertes financières directes.

Riskwares

Niveau de danger : bas

Les riskwares appartiennent à la catégorie des programmes potentiellement dangereux (catégorie not-a-virus). Ces programmes peuvent être vendus légalement et utilisés dans le travail quotidien, par exemple par les administrateurs de réseau.

La catégorie des riskwares reprend par exemple certains programmes d'administration à distance tels que RemoteAdmin. L'utilisateur installe et exécute lui-même ces programmes sur son ordinateur. Cette caractéristique les distingue des chevaux de Troie d'administration à distance (Backdoor) qui s'installent eux-mêmes dans le système et qui le gèrent à l'insu de l'utilisateur.

Cette catégorie de programme contient par exemple certains programmes de permutation automatique de la disposition du clavier, des clients IRC, des serveurs FTP, des utilitaires d'arrêt de processus ou de dissimulation de leur fonctionnement.

1.1.3. Présentation des objets infectés, suspects et potentiellement dangereux

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

Si Kaspersky Anti-Virus découvre dans l'objet analysé une portion de code qui correspond parfaitement à la portion de code de contrôle d'une menace quelconque (selon les informations présentes dans la base), il attribue à l'objet l'état *infecté*. Si l'équivalence n'est que partielle (en fonction de circonstances définies), il lui donne l'état *suspect*.

Kaspersky Anti-Virus reconnaît également les *objets présentant un risque potentiel*. Pour ce faire, il utilise l'analyseur heuristique (Code Analyzer). Il n'est pas possible de définir si le code de cet objet correspond partiellement ou parfaitement au code d'une menace connue mais par contre, il contient des séquences de commande propres aux objets malveillants telles que l'ouverture ou l'écriture dans un fichier ou l'interception de vecteurs d'interruption. L'analyseur heuristique décide, par exemple, que le fichier semble être infecté par un virus de démarrage connu.

Si Kaspersky Anti-Virus détermine qu'un objet est infecté ou suspect, il renvoie le nom de la menace découverte ; si Kaspersky Anti-Virus estime que l'objet présente un risque potentiel, il ne renvoie pas de nom de menace.

Remarque

Dans la fenêtre de configuration des paramètres de sécurité et dans les boîtes de dialogue **Statistiques** de la console de Kaspersky Anti-Virus, l'expression *objets présentant un risque potentiel* n'est pas utilisée : Kaspersky Anti-Virus applique le terme *suspect* aux objets présentant un risque potentiel et aux objets vraiment suspects (dont le code contient des segments qui correspondent en partie au code d'une menace connue).

Dans les autres boîtes de dialogues de la console de Kaspersky Anti-Virus, les expressions *objets suspects* et *objets présentant un risque potentiel* sont cités séparément. L'expression *objets suspects* désigne uniquement les objets suspects.

1.2. Informations relatives à Kaspersky Anti-Virus

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Anti-Virus, vous pouvez obtenir la réponse rapidement.

Kaspersky Lab propose à cette fin plusieurs sources d'informations sur l'application et vous pouvez sélectionner celle qui vous convient le mieux en fonction de l'importance et de l'urgence de votre question. Vous pouvez :

- Trouver vous-même la réponse à votre question (cf. point 1.2.1, p. 22) ;
- Obtenir une réponse des agents commerciaux du service des ventes (cf. point 1.2.2, p. 24) ;
- Obtenir une réponse de l'agent du service d'assistance technique si vous avez déjà acheté Kaspersky Anti-Virus (cf. point 1.2.3, p. 24) ;

- Discuter de votre question non seulement avec des experts de Kaspersky Lab mais également avec d'autres utilisateurs dans le forum consacré à Kaspersky Anti-Virus (cf. point 1.2.4, p. 26).

1.2.1. Sources d'informations pour une recherche indépendante

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

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

Page sur le site de Kaspersky Lab

http://www.kaspersky.com/fr/kaspersky_anti-virus_windows_server_enterprise

Cette page vous propose des informations générales sur l'application, ses possibilité et ses particularités. Vous pouvez acheter l'application ou prolonger la licence dans notre magasin en ligne.

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

http://kb.kaspersky.fr/article/entreprises/1584.html

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

Ces articles contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. Ils sont regroupés par sujets tels que « Manipulation des fichiers de clé », « Configuration de la mise à jour des bases » ou « Dépannage de l'application ». Les articles peuvent répondre à des question qui ne se rapportent pas uniquement à cette applications mais à d'autres logiciels de Kaspersky Lab également ; ils peuvent contenir des nouvelles sur le Service d'assistance technique dans son ensemble.

Système d'aide électronique

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

L'aide complète contient les informations sur l'administration de la protection de l'ordinateur à l'aide de la console de Kaspersky Anti-Virus dans MMC : consultation de l'état de la protection, exécution de l'analyse de divers secteurs de l'ordinateur, exécution d'autres tâches. Elle explique également comment administrer l'application via la ligne de commande, comment utiliser les compteurs de performance de Kaspersky Anti-Virus ou les compteurs et les pièges du protocole SNMP.

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

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

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

Documentation

La série de documents qui accompagne l'application contient la majorité des informations nécessaires à l'utilisation du logiciel. Elle est composée des documents suivants :

- **Schémas types de déploiement**. Ce document présente le déploiement de Kaspersky Anti-Virus dans le réseau de l'entreprise.
- **Comparaison avec Kaspersky Anti-Virus 6.0 for Windows Servers**. Ce document énumère les caractéristiques de Kaspersky Anti-Virus qui le distingue de Kaspersky Anti-Virus 6.0 for Windows Servers.
- **Le Guide d'installation** contient les configurations matérielle et logicielle requises pour l'installation de Kaspersky Anti-Virus, les instructions pour l'installation et l'activation du logiciel, la marche à suivre pour vérifier son fonctionnement et procéder à la configuration initiale.
- **Le guide de l'administrateur** (ce document) contient les informations sur l'utilisation de la console de Kaspersky Anti-Virus dans MMC, l'administration de Kaspersky Anti-Virus depuis Kaspersky Administration Kit ou via la ligne de commande, l'utilisation des compteurs de performance de Kaspersky Anti-Virus et des compteurs et des pièges pour le protocole SNMP.

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

Vous pouvez également les télécharger depuis la page de l'application sur le site de Kaspersky Lab.

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

1.2.2. Contacter le service ventes

Si vous avez des questions sur la sélection ou l'achat de Kaspersky Anti-Virus ou sur la prolongation de la licence, vous pouvez contacter les agents commerciaux du service vente de notre siège central à Moscou un composant un des numéros de téléphone suivants :

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

Le service est offert en russe et en anglais.

Vous pouvez également contacter les agents commerciaux du service ventes en écrivant à sales@kaspersky.com.

Le service ventes peut vous aider dans le domaine de l'administration de la protection du réseau de l'entreprise, du déploiement de l'application ou de son utilisation avec d'autres applications.

1.2.3. Contacter le service d'assistance technique

Si vous avez déjà acheté l'application, vous pouvez obtenir des informations auprès des experts du service d'assistance technique par téléphone ou via Internet.

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et vous aideront à réparer les dégâts provoqués par des programmes malveillants si votre ordinateur est déjà infecté.

Assistance technique par téléphone

Si le problème est urgent, vous pouvez toujours contacter le service d'assistance technique par téléphone dans notre bureau de Moscou en composant le :

+7 (495) 797-87-07, **+7 (495) 645-79-29** ou **+7 (495) 956-87-08**.

L'assistance téléphonique est offerte aux utilisateurs des applications de Kaspersky Lab en russe et en anglais 24h/24.

Si vous souhaitez parler à un expert spécialisé dans l'application « Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition », contactez le service les jours ouvrables entre 10h et 18h30 (heure de Moscou, GMT+3).

Communiquez à l'opérateur du service d'assistance technique le **code d'activation** de l'application ou le **numéro de série de la clé** (vous le trouverez dans le noeud **Clé** de la console de Kaspersky Anti-Virus, dans les propriétés de la clé installée).

Requête électronique adressée au service d'assistance technique (pour les utilisateurs enregistrés)

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

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

Pour envoyer une requête électronique, vous devez saisir le **numéro de client** que vous avez obtenu lors de votre enregistrement sur le site du service d'assistance technique et votre **mot de passe**.

Remarque

Si vous n'êtes pas encore un utilisateur enregistré des applications de Kaspersky Lab, vous pouvez remplir le formulaire d'enregistrement à la page :

https://support.kaspersky.com/ru/PersonalCabinet/Registration/Form/?LANG=fr

Lors de l'enregistrement, indiquez le **code d'activation** de l'application ou le **numéro de série de la clé** (vous le trouverez dans le nœud **Clé** de la console de Kaspersky Anti-Virus, dans les propriétés de la clé installée).

Le spécialiste du service d'assistance technique enverra la réponse à votre requête à l'adresse de messagerie que vous aviez indiquée et à votre **Casier personnel**

https://support.kaspersky.com/ru/PersonalCabinet?LANG=fr.

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

- **Le type de requête**. Les questions que les utilisateurs posent le plus souvent sont regroupées en thèmes séparés, par exemple « Problème d'installation/de suppression du logiciel » ou « Problème de recherche/de neutralisation de virus ». Si vous ne trouvez pas le thème qui se rapporte à votre cas, choisissez « Question générale ».
- **Logiciel** : Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.

- **Le texte du message**. Décrivez avec le plus de détail possible le problème rencontré.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement sur le site du service d'assistance technique de Kaspersky Lab.
- **Courrier électronique**. Les experts du service d'assistance technique enverront leurs réponses à cette adresse.

1.2.4. Discussion sur les applications de Kaspersky Lab dans le forum

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

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

Vous pouvez, par exemple, débattre des diverses méthodes de déploiement de l'application dans une entreprise ou de ses diverses configurations.

PARTIE 1. CONFIGURATION ET ADMINISTRATION VIA LA CONSOLE MMC

Cette section aborde les sujets suivants :

- Lancement de la console de Kaspersky Anti-Virus dans MMC, accès aux fonctions de Kaspersky Anti-Virus, description de l'apparence de la fenêtre de la console (cf. Chapitre 2, p. 28) ;
- Configuration des paramètres généraux de Kaspersky Anti-Virus (cf. Chapitre 3, p. 45) ;
- Importation et exportation des paramètres de Kaspersky Anti-Virus et de ses composants (cf. Chapitre 4, p. 50) ;
- Concept de tâche dans Kaspersky Anti-Virus, type de tâche, manipulation des tâches, programmation de l'exécution des tâches, consultation des statistiques des tâches, exécution des tâches sous les privilèges d'un autre compte (cf. Chapitre 5, p. 54) ;
- Configuration de la protection en temps réel du serveur(cf. Chapitre 6, p. 68) ;
- Interdiction de l'accès des ordinateurs au serveur pendant l'exécution de la tâche Protection en temps réel des fichiers (cf. Chapitre 7, p. 97) ;
- Zone de confiance (cf. Chapitre 8, p. 109) ;
- Configuration de l'analyse à la demande (cf. Chapitre 9, p. 121) ;
- Actualisation des bases de Kaspersky Anti-Virus et de ses modules (cf. Chapitre 10, p. 151) ;
- Utilisation de la quarantaine pour isoler les objets suspects (cf. Chapitre 11, p. 171) ;
- Sauvegarde des fichiers avant la réparation ou la suppression, utilisation de la sauvegarde (cf. Chapitre 12, p. 190) ;
- Consignation des événements et statistiques de Kaspersky Anti-Virus (cf. Chapitre 13, p. 204) ;
- Installation et suppression des clés (cf. Chapitre 14, p. 230) ;
- Configuration des notifications (cf. Chapitre 15, p. 236).

CHAPITRE 2. UTILISATION DE LA CONSOLE DE KASPERSKY ANTI-VIRUS DANS MMC ET ACCES AUX SES FONCTIONS

Le présent chapitre aborde les sujets suivants :

- Présentation de la console de Kaspersky Anti-Virus dans MMC (cf. point 2.1, p. 28) ;
- Configuration avancée après l'installation de la console de Kaspersky Anti-Virus dans MMC sur un autre ordinateur (cf. point 2.2, p. 29) ;
- Lancement de la console de Kaspersky Anti-Virus au départ du menu Démarrer (cf. point 2.3, p. 35) ;
- Fonctions de l'icône de Kaspersky Anti-Virus dans la zone de notification la barre des tâches du serveur protégé (cf. point 2.4, p. 36) ;
- Apparence de la fenêtre de la console de Kaspersky Anti-Virus (cf. point 2.5, p. 38) ;
- Restriction des privilèges d'accès aux fonctions de Kaspersky Anti-Virus (cf. point 2.6, p. 38) ;
- Lancement et arrêt du service de Kaspersky Anti-Virus (cf. point 2.7, p. 44).

2.1. Présentation de la console de Kaspersky Anti-Virus dans MMC

La console de Kaspersky Anti-Virus est un composant enfichable isolé qui est ajouté à la console MMC (Microsoft Management Console).
Une fois l'installation de la console de Kaspersky Anti-Virus terminée, le programme d'installation conserve le fichier kavfs.msc dans le répertoire de Kas-

persky Anti-Virus et ajoute le composant enfichable à la liste des composants isolés de Microsoft Windows.
Vous pouvez ouvrir la console d'administration de Kaspersky Anti-Virus sur le serveur protégé à l'aide du menu Démarrer ou depuis le menu contextuel de l'icône de Kaspersky Anti-Virus  dans la zone de notification la barre des tâches, en exécutant le fichier msc avec le composant enfichable ou en ajoutant le composant enfichable Kaspersky Anti-Virus dans la console existante en tant que nouvel élément de l'arborescence.
Il est possible d'administrer Kaspersky Anti-Virus via la console dans MMC installée sur le serveur protégé ou sur n'importe quel autre poste du réseau. Après avoir installé la console de Kaspersky Anti-Virus sur un autre ordinateur, vous devez procéder à une configuration avancée décrite au point 2.2 à la page 29.
Dans une console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants enfichables Kaspersky Anti-Virus afin de pouvoir administrer ainsi la protection de plusieurs serveur sur lesquels Kaspersky Anti-Virus est installé.

2.2. Configuration avancée après l'installation de la console de Kaspersky Anti-Virus dans MMC sur un autre ordinateur

Si vous avez installé la console de Kaspersky Anti-Virus dans MMC non pas sur le serveur à protéger mais sur un autre ordinateur, alors afin de pouvoir administrer Kaspersky Anti-Virus à distance sur le serveur protégé, il faudra réaliser les actions suivantes :

- ajoutez les utilisateurs de Kaspersky Anti-Virus au groupe **KAVWSEE Administrators** sur le serveur protégé (cf. point 2.2.1, p. 30) ;
- si le serveur protégé tourne sous Microsoft Windows Server 2008, alors autorisez les connexions de réseau pour le service d'administration de Kaspersky Anti-Virus kavfsgt.exe (cf. point 2.2.2, p. 31) ;
- si l'ordinateur distant tourne sous Microsoft Windows XP avec Service Pack 1 ou 2 ou sous Windows Vista, ouvrez les connexions de réseau entre la console de Kaspersky Anti-Virus dans MMC et le service d'administration de Kaspersky Anti-Virus (cf. point 2.2.3, p. 32).
- si l'ordinateur distant fonctionne sous Microsoft Windows XP Service Pack 1, désactivez le pare-feu Windows afin d'ouvrir les connexions de réseau pour la console de Kaspersky Anti-Virus installée (cf. point. 2.2.3, p. 32) ;

- Pour la console de Kaspersky Anti-Virus sur un ordinateur tournant sous Microsoft Windows XP Service Pack 2 ou Microsoft Windows Vista : si au moment d'installer la console, vous n'avez pas coché la case **Autoriser les connexions de réseau pour la console de Kaspersky Anti-Virus**, alors autorisez manuellement les connexions de réseau pour la console via le pare-feu sur cet ordinateur (cf. point 2.2.4, p. 33).

2.2.1. Ajout d'utilisateurs de Kaspersky Anti-Virus au groupe KAVWSEE Administrators sur le serveur protégé

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

Remarque

Pour connaître les services enregistrés par Kaspersky Anti-Virus, lisez le document *Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition. Manuel d'installation*.

Vous pouvez octroyer l'accès au service d'administration de Kaspersky Anti-Virus aux comptes utilisateur des types suivants :

- **Comptes utilisateur enregistrés localement** sur l'ordinateur où est installée la console de Kaspersky Anti-Virus. Pour établir la connexion, un compte utilisateur avec les mêmes données doit être enregistré localement sur le serveur protégé ;
- **Comptes utilisateur enregistrés dans le domaine** où est enregistré l'ordinateur doté de la console de Kaspersky Anti-Virus. Pour établir la connexion, le serveur protégé doit être enregistré dans le même domaine ou dans un domaine situé dans des rapports de confiance avec ce domaine.

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

Pour octroyer ou refuser l'accès au service d'administration de Kaspersky Anti-Virus :

1. Sur le serveur protégé, sélectionnez **Démarrer** → **Paramètres** → **Panneau de configuration**. Dans la fenêtre **Panneau de configuration**, sélectionnez **Administration** → **Administration de l'ordinateur**.
2. Dans l'arborescence de la console **Administration de l'ordinateur**, déployez le nœud **Utilisateurs et groupes locaux** puis, déployez le nœud **Groupes**.
3. Cliquez deux fois sur le groupe **KAVWSEE Administrators** et dans la boîte de dialogue **Propriétés**, exécutez les actions suivantes :
   - Pour autoriser un utilisateur à procéder à l'administration à distance de Kaspersky Anti-Virus à l'aide de la console, ajoutez-le au groupe **KAVWSEE Administrators** ;
   - Pour interdire à un utilisateur l'administration à distance de Kaspersky Anti-Virus à l'aide de la console, retirez-le du groupe **KAVWSEE Administrators**.
4. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés**.

2.2.2. Autorisation des connexions de réseau sous un serveur tournant sous Microsoft Windows Server 2008 pour le service d'administration de Kaspersky Anti-Virus

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

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

1. Sur le serveur protégé tournant sous Microsoft Windows Server 2008, sélectionnez **Démarrer** → **Panneau de configuration** → **Sécurité** → **Pare-feu Windows**.
2. Dans la fenêtre **Paramètres du pare-feu Windows**, cliquez sur **Modifier les paramètres**.

3. Sur l'onglet **Exclusions**, dans la liste des exclusions prédéfinies, cochez les cases **COM + Accès réseau**, **Windows Management Instrumentation (WMI)** et **Remote Administration**.
4. Cliquez sur le bouton **Ajouter programme**.
5. Dans la boîte de dialogue **Ajout d'un programme**, sélectionnez le fichier kavfsgt.exe. Il se trouve dans le répertoire que vous avez sélectionné lors de l'installation de la console de Kaspersky Anti-Virus dans MMC. Par défaut, le chemin d'accès complet au fichier est le suivant :
   - dans la version 32 bits de Microsoft Windows : %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe ;
   - dans la version 64 bits de Microsoft Windows : %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe.
6. Cliquez sur **OK**.
7. Cliquez sur **OK** dans la boîte de dialogue **Paramètres du pare-feu Windows**.

2.2.3. Autorisation des connexions de réseau pour la console de Kaspersky Anti-Virus dans MMC sous Microsoft Windows XP avec Service Pack 1

Si l'ordinateur sur lequel la console de Kaspersky Anti-Virus est installée tourne sous Microsoft Windows XP avec Service Pack 1, il faudra désactiver le pare-feu sur cet ordinateur pour autoriser les connexions de réseau pour la console :

1. Sur l'ordinateur sur lequel est installé la console de Kaspersky Anti-Virus dans MMC, sélectionnez **Démarrer** → **Panneau de configuration** → **Connexions de réseau**.
2. Ouvrez le menu contextuel du nom de la connexion de réseau (par exemple, **Local Area Connection**) et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **<Nom de la connexion de réseau>: Propriétés**, sous l'onglet **Avancé**, désélectionnez la case **Protéger ma connexion à Internet**.
4. Cliquez sur **OK**.

2.2.4. Autorisation des connexions de réseau pour la console de Kaspersky Anti-Virus dans MMC sous Microsoft Windows XP avec Service Pack 2 ou Microsoft Windows Vista

La console de Kaspersky Anti-Virus dans MMC sur l'ordinateur distant utilise le protocole DCOM afin d'obtenir des informations sur les événements de Kaspersky Anti-Virus (objets analysés, tâches terminées, etc.) fournies par le service d'administration de Kaspersky Anti-Virus sur le serveur protégé.

Si l'ordinateur sur lequel est installée la console tourne sous Microsoft Windows XP avec Service Pack 2 ou Microsoft Windows Vista, vous devrez autoriser les connexions de réseau via le pare-feu sur cet ordinateur afin d'établir des connexions entre la console et le service d'administration de Kaspersky Anti-Virus.

Exécutez les actions suivantes :

- Assurez-vous que l'accès à distance anonyme aux applications COM est autorisé (mais pas le lancement à distance et l'activation des applications COM) .
- Dans le pare-feu Windows, ouvrez le port TCP 135 et autorisez les connexions de réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Anti-Virus.
- Le port TCP 135 est utilisé par l'ordinateur sur lequel la console de Kaspersky Anti-Virus est installée dans MMC pour communiquer avec le serveur protégé et le serveur répond à cette requête par ce même port.

Pour autoriser l'accès anonyme à distance aux applications COM :

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

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

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

1. Sur l'ordinateur distant, ouvrez la console de Kaspersky Anti-Virus dans MMC.
2. Exécutez une des actions suivantes :
   - dans *Microsoft Windows XP Service Pack 2 ou suivant*, sélectionnez **Démarrer → Panneau de configuration → Pare-feu Windows**.
   - dans *Microsoft Windows Vista*, sélectionnez **Démarrer → Panneau de configuration → Pare-feu Windows** et dans la fenêtre **Pare-feu Windows**, cliquez sur **Modifier les paramètres**.
3. Sur l'onglet **Exclusions** de la fenêtre **Pare-feu Windows**, cliquez sur le bouton **Ajouter port**.
4. Dans le champ **Nom**, indiquez le nom du port **RPC (TCP/135)** ou définissez un autre nom, par exemple **DCOM Kaspersky Anti-Virus** et dans le champ **Numéro de port**, indiquez le numéro du port : **135**.
5. Sélectionnez le protocole **TCP**.
6. Cliquez sur **OK**.
7. Sur l'onglet **Exclusions**, cliquez sur le bouton **Ajouter programme**.
8. Dans la boîte de dialogue **Ajout de programme**, indiquez le fichier kavfsrcn.exe. Il se trouve dans le répertoire que vous avez choisi en tant que répertoire cible pour l'installation de la console de Kaspersky Anti-Virus dans MMC. Le chemin d'accès complet par défaut est le suivant :
   - dans la *version 32 bits de Microsoft Windows* : %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe ;
   - *dans Microsoft Windows version 64 bits* : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.
9. Cliquez sur **OK**.

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

> **Remarque**
>
> *Pour appliquer de nouveaux paramètres de connexion :* si la console de Kaspersky Anti-Virus était ouverte pendant que vous configuriez la connexion entre le serveur protégé et l'ordinateur sur lequel la console est installée, fermez la console, attendez entre 30 et 60 secondes (pour laisser le temps au processus d'administration à distance de Kaspersky Anti-Virus kavfsrcn.exe de s'arrêter) puis relancez-la.

2.3. Lancement de la console de Kaspersky Anti-Virus depuis le menu *Démarrer*

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

1. Pour ouvrir la console de Kaspersky Anti-Virus depuis le menu **Démarrer**, sélectionnez **Démarrer** → **Programmes** → **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Outils d'administration** → **Console de Kaspersky Anti-Virus**

> **Remarque**
>
> Si vous avez l'intention d'ajouter d'autres composants enfichables à la console de Kaspersky Anti-Virus, ouvrez la console en mode édition : sélectionnez **Démarrer** → **Programmes** → **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Outils d'administration**, ouvrez le menu contextuel de l'application **Console de Kaspersky Anti-Virus**et sélectionnez **Auteur**.

Si vous avez lancé la console de Kaspersky Anti-Virus sur le serveur protégé, la fenêtre de la console s'ouvre (cf. ill. 1).

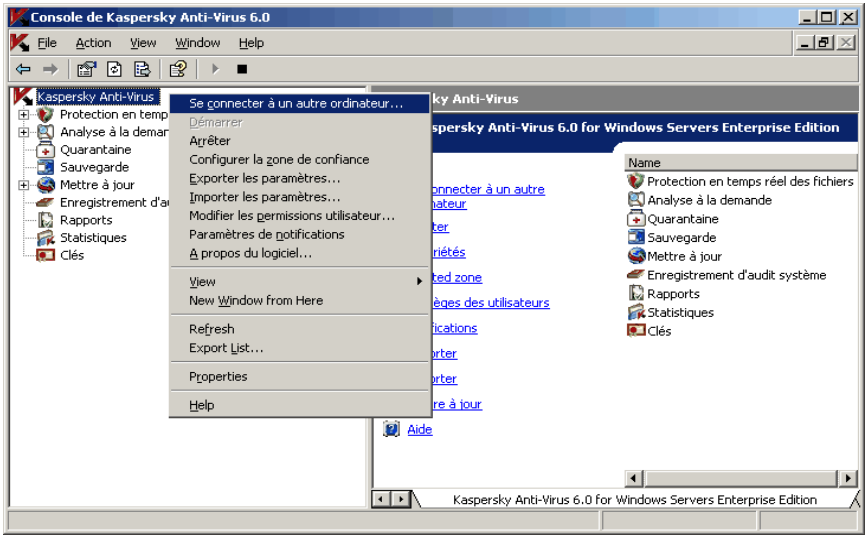

Illustration 1. Fenêtre de la console de Kaspersky Anti-Virus

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

   Si le compte utilisateur employé pour accéder à Microsoft Windows ne jouit pas des privilèges d'accès au service d'administration de Kaspersky Anti-Virus sur le serveur, indiquez un autre compte qui jouit de ces privilèges. Pour obtenir de plus amples informations sur les comptes utilisateurs qui peuvent jouir de l'accès au service d'administration de Kaspersky Anti-Virus, consultez le point 2.2.1 à la page 30.

2.4. Icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches

Chaque fois que Kaspersky Anti-Virus s'ouvre automatiquement après le redémarrage du serveur, son icône apparaît dans la zone de notification de la

barre des tâches du serveur. Elle est affichée par défaut si le composant **Application de la barre des tâches** a été inclus dans la sélection des composants installés avec Kaspersky Anti-Virus.

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

- Actif (en couleur) si un des tâches de protection en temps réel est en cours d'exécution : **Protection en temps réel des fichiers** ou l'**Analyse des scripts** (pour en savoir plus sur les tâches de protection en temps réel, lisez le point 6.1 à la page 68) ;
- Inactif (noir et blanc) si la **Protection en temps réel des fichiers** ou l'**Analyse des scripts** n'est pas exécutée à ce moment.

Un clic du bouton gauche de la souris sur l'icône de Kaspersky Anti-virus permet d'ouvrir le menu contextuel présenté dans l'illustration 2.

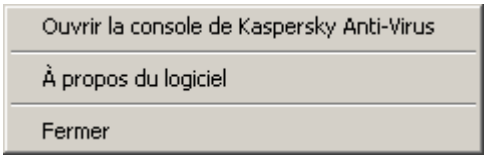

Illustration 2. Menu contextuel de l'icône de Kaspersky Anti-Virus

Le menu contextuel contient les commandes suivantes :

Commande	Description
Ouvrir console de Kaspersky Anti-Virus	Ouvre la console de Kaspersky Anti-Virus dans MMC (si elle est installée).
À propos du logiciel	Ouvre la fenêtre **À propos du logiciel** qui contient des informations sur Kaspersky Anti-Virus Si vous êtes un utilisateur enregistré de Kaspersky Anti-Virus, alors la fenêtre **À propos du logiciel** contient des informations sur les mises à jour urgentes installées.
Masquer	Cache l'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches. Pour afficher l'icône de Kaspersky Anti-Virus, dans le menu **Démarrer** sélectionnez **Programmes** → **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** → **Applications de la barre des tâches**.

Dans les paramètres généraux de Kaspersky Anti-Virus, vous pouvez activer ou désactiver l'affichage de l'icône de Kaspersky Anti-Virus à l'ouverture automatique de Kaspersky Anti-Virus après un redémarrage du serveur (cf. point 3.2, p. 46).

2.5. Fenêtre de la console de Kaspersky Anti-Virus

La fenêtre de la console de Kaspersky Anti-Virus (cf. ill. 3) contient l'arborescence de la console et le panneau des résultats. L'arborescence reprend les nœuds des composants de Kaspersky Anti-Virus tandis que le panneau des résultats affiche les informations relatives au nœud sélectionné.

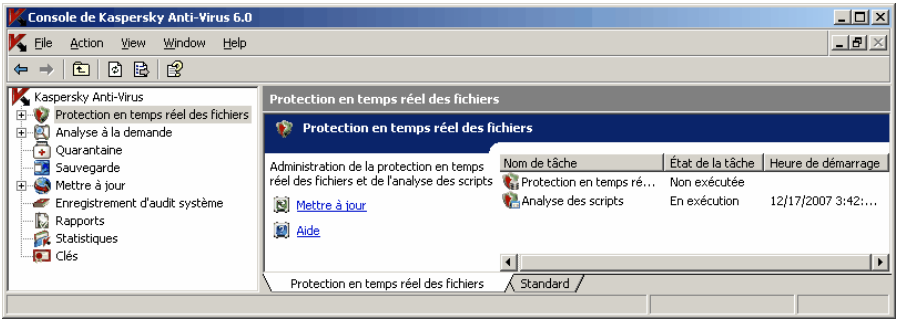

Illustration 3. Console de Kaspersky Anti-Virus

La fenêtre de la console de Kaspersky Anti-Virus contient également le panneau des tâches si vous l'avez lancée depuis le menu **Démarrer** (depuis le fichier msc enregistré lors de l'installation de Kaspersky Anti-Virus). Si vous avez ajouté le composant enfichable Kaspersky Anti-Virus dans la console MMC existante, alors la console ne propose pas le panneau des tâches.

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

Cette section aborde les sujets suivants :

- Présentation des privilèges d'accès aux fonctions de Kaspersky Anti-Virus (cf. point 2.6.1, p. 39) ;
- Configuration des privilèges d'accès aux fonctions de Kaspersky Anti-Virus (cf. point 2.6.2, p. 41).

2.6.1. Présentation des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

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

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

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

Vous pouvez octroyer aux utilisateurs de Kaspersky Anti-Virus (groupe) des privilèges d'accès à :

- L'ensemble des fonctions de Kaspersky Anti-Virus (**contrôle total**) ;
- L'ensemble des fonctions de Kaspersky Anti-Virus, à l'exception de la fonction d'administration des privilèges des utilisateurs (**modification**) ;
- Consultation uniquement des composants fonctionnels de Kaspersky Anti-Virus, des paramètres généraux de Kaspersky Anti-Virus, des paramètres de ses tâches et de ses fonctions, des statistiques et des privilèges des utilisateurs (**lecture**).

Vous pouvez également procéder à une configuration étendue des privilèges d'accès : autoriser ou interdire l'accès aux fonctions individuelles de Kaspersky Anti-Virus. Les fonctions dont vous pouvez administrer l'accès sont reprises dans le tableau 1.

Tableau 1. Restriction des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

Fonction	Description
Consultation des statistiques	Consultation de l'état des composants fonctionnels de Kaspersky Anti-Virus et des statistiques sur les tâches en cours
Administration de l'état des tâches	Lancement / arrêt/ suspension / rétablissement des tâches de Kaspersky Anti-Virus
Gérer les tâches	Création et suppression de tâches d'analyse à la demande
Lire les paramètres	• Consultation des paramètres généraux de Kaspersky Anti-Virus et des paramètres des tâches ; • Consultation des paramètres des rapports, des notifications et de l'audit système ; • Exportation des paramètres de Kaspersky Anti-Virus
Modifier les paramètres	• Consultation et modification des paramètres généraux de Kaspersky Anti-Virus ; • Importation et exportation des paramètres de Kaspersky Anti-Virus ; • Consultation et modification des paramètres des tâches ; • Consultation et modification des paramètres des rapports, des notifications et de l'audit système
Gérer la quarantaine et les sauvegardes	• Placement des objets en quarantaine ; • Suppression des objets de la quarantaine et des fichiers de la sauvegarde ; • Récupération des objets de la sauvegarde et de la quarantaine
Lire les rapports	Consultation des rapports détaillés et de synthèse sur l'exécution des tâches dans le nœud **Rapports** et sur les événements dans le nœud **Enregistrement d'audit système**
Gérer les rapports	Suppression des rapports et purge du journal d'audit système

Fonction	Description
Gérer les clés de licence	Installation et suppression des clés
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Anti-Virus
Modification des privilèges	• Ajout et suppression d'utilisateurs de Kaspersky Anti-Virus ; • Modification des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

2.6.2. Configuration des privilèges d'accès aux fonctions de Kaspersky Anti-Virus

Pour ajouter un utilisateur (groupe) ou le supprimer ou pour modifier les privilèges d'accès de l'utilisateur (du groupe) :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du composant enfichable Kaspersky Anti-Virus et sélectionnez le point **Modifier les privilèges des utilisateurs**.

   La boîte de dialogue **Autorisations** s'ouvre (cf. ill. 4).

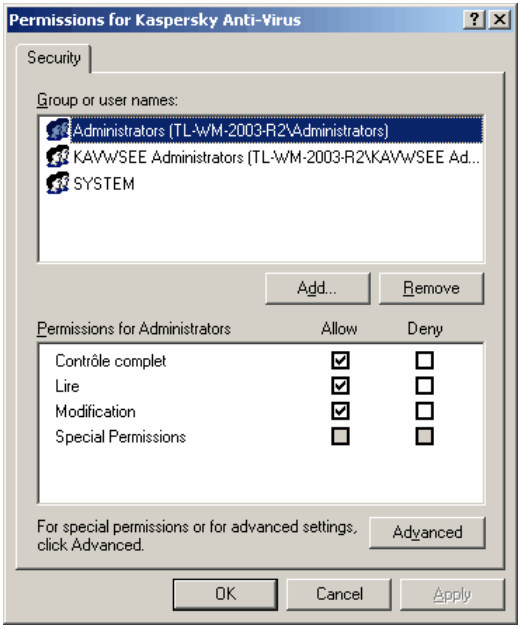

Illustration 4. Boîte de dialogue **Autorisations**

2. Exécutez les actions suivantes dans la fenêtre **Autorisations** :

   - Pour ajouter un utilisateur (un groupe) à la liste des utilisateurs de Kaspersky Anti-Virus, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe que vous souhaitez ajouter ;
   - Pour octroyer à l'utilisateur (au groupe) ajouté des privilèges d'accès aux fonctions de Kaspersky Anti-Virus, sélectionnez l'utilisateur (le groupe) sous le titre **Groupes ou utilisateurs** et sous le titre **Autorisations pour <Utilisateur (Groupe)>**, cochez la case **Autoriser** en regard des privilèges suivants :
     - **Contrôle complet** pour octroyer l'accès à toutes les fonctions de Kaspersky Anti-Virus ;
     - **Lecture** pour octroyer l'accès aux fonctions. **Lire les statistiques**, **Lire les paramètres**, **Lire les paramètres** et **Lecture des privilèges** ;
     - **Modification** pour octroyer l'accès à l'ensemble des fonctions de Kaspersky Anti-Virus, sauf **Modification des privilèges**.

- Pour procéder à la configuration étendue des privilèges (**Autorisations spéciales**), cliquez sur le bouton **Avancé**, dans la boîte de dialogue **Paramètres de sécurité complémentaires** sélectionnez l'utilisateur ou le groupe requis et cliquez sur **Modifier**. Ensuite, dans la boîte de dialogue **Eléments d'autorisation** (cf. ill. 5) cochez la case **Autoriser** ou **Interdire** à côté du nom de la fonction dont vous souhaitez autoriser ou interdire l'accès (la liste des fonctions et une brève description figurent au tableau 1). Cliquez sur **OK**.

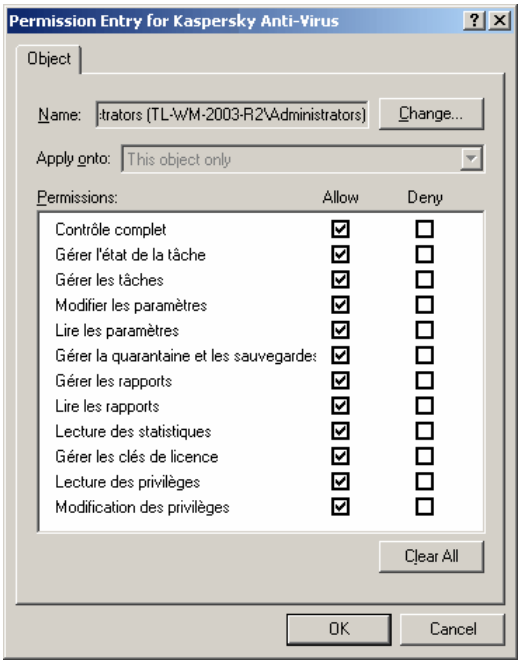

Illustration 5. Boîte de dialogue **Elément d'autorisation**

3. Cliquez sur le bouton **OK** dans la boîte de dialogue **Autorisations**.

2.7. Lancement et arrêt du service de Kaspersky Anti-Virus

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

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

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

Remarque

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

Pour arrêter ou lancer le service de Kaspersky Anti-Virus, ouvrez le menu contextuel du composant enfichable Kaspersky Anti-Virus dans l'arborescence de la console et choisissez une des commandes suivantes :

- **Arrêter** pour arrêter le service de Kaspersky Anti-Virus ;
- **Démarrer** pour lancer le service de Kaspersky Anti-Virus.

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

CHAPITRE 3. PARAMETRES GENERAUX DE KASPERSKY ANTI-VIRUS

Le présent chapitre aborde les sujets suivants :

- Présentation des paramètres généraux de Kaspersky Anti-Virus (cf. point 3.1, p. 45) ;
- Configuration des paramètres généraux de Kaspersky Anti-Virus (cf. point 3.2, p. 46).

Une description des paramètres généraux de Kaspersky Anti-Virus est proposée au point B.1 à la page 376.

3.1. Présentation des paramètres généraux de Kaspersky Anti-Virus

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

3.2. Configuration des paramètres généraux de Kaspersky Anti-Virus

Cette rubrique contient les informations relatives à la configuration des paramètres généraux de Kaspersky Anti-Virus. Une description des paramètres généraux est proposée au point B.1 à la page 376.

Pour configurer les paramètres généraux de Kaspersky Anti-Virus :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du composant enfichable Kaspersky Anti-Virus et sélectionnez le point **Propriétés**.
2. Sur les onglets suivants, modifiez la valeur des paramètres généraux de Kaspersky Lab en fonction de vos besoins.
   - Sur l'onglet **Général** (cf. ill. 6) :
     - Définissez le nombre maximum de processus actifs que Kaspersky Anti-Virus peut lancer (cf. ill. B.1.1, p. 377) ;
     - Définissez le nombre de processus fixe pour les tâches de la protection en temps réel (cf. point B.1.2, p. 378) ;
     - Définissez le nombre de processus actifs pour les tâches d'analyse à la demande en arrière-plan (cf. point B.1.3, p. 379) ;
     - Définissez le nombre de tentatives de restauration des tâches après un arrêt accidentel de celles-ci (cf. point B.1.4, p. 380).

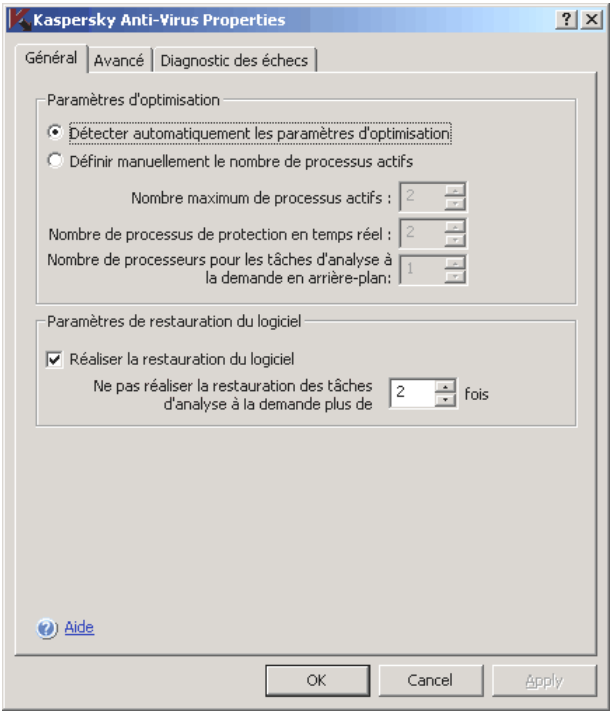

Illustration 6. Boîte de dialogue **Propriétés**, onglet **Général**

- Sur l'onglet **Avancé** (cf. ill. 7) :
  - Indiquez s'il faut afficher ou non l'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches du serveur chaque fois que Kaspersky Anti-Virus est ouvert après le redémarrage du serveur (pour de plus amples informations sur l'icône de Kaspersky Anti-Virus, consultez le point. 2.4 à la page 36) ;
  - Indiquez la durée (en jours) pendant laquelle les rapports de synthèse et détaillés sur l'exécution des tâches repris dans le nœud **Rapports** de la console de Kaspersky Anti-Virus seront conservés (cf. point B.1.5, p. 381) ;
  - Indiquez la durée de conservation, en jours, des informations affichées dans le nœud **Enregistrement d'audit système** (cf. point B.1.6, p. 382) ;

- Indiquez les actions exécutées par Kaspersky Anti-Virus en cas d'alimentation par la batterie (cf. B.1.7, p. 383) ;
- Définissez le nombre de jours après lequel les événements *La base de données n'est plus à jour*, *La base de données est périmée* et *L'analyse complète de l'ordinateur n'a pas été réalisée depuis longtemps* sont déclenchés (cf. point B.1.8 p. 383).

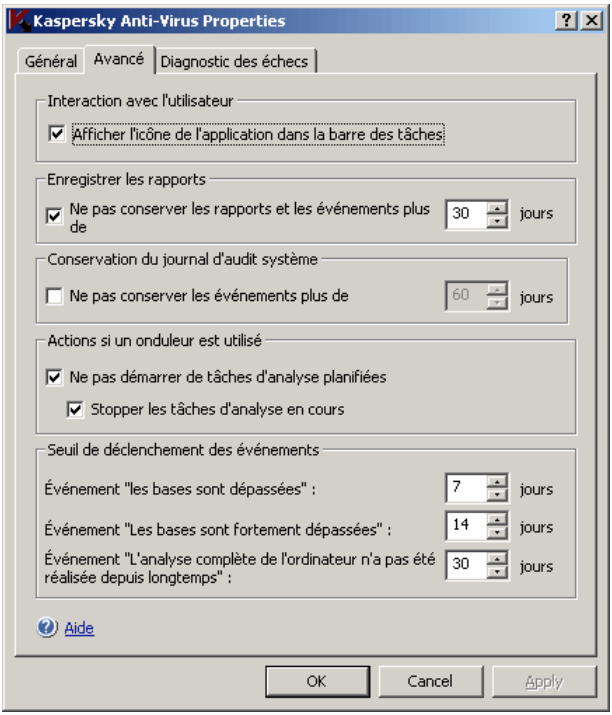

Illustration 7. Boîte de dialogue **Propriétés**, onglet **Avancé**

- Sur l'onglet **Diagnostic des échecs** (cf. ill. 8) :
  - Activez ou désactivez la constitution d'un journal de traçage (la case **Consigner les informations de débogage dans le fichier**) ; le cas échéant, configurer les paramètres du journal (cf. point B.1.9, p. 384) ;
  - Activez ou désactivez la création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (cf. point B.1.10, p. 390).

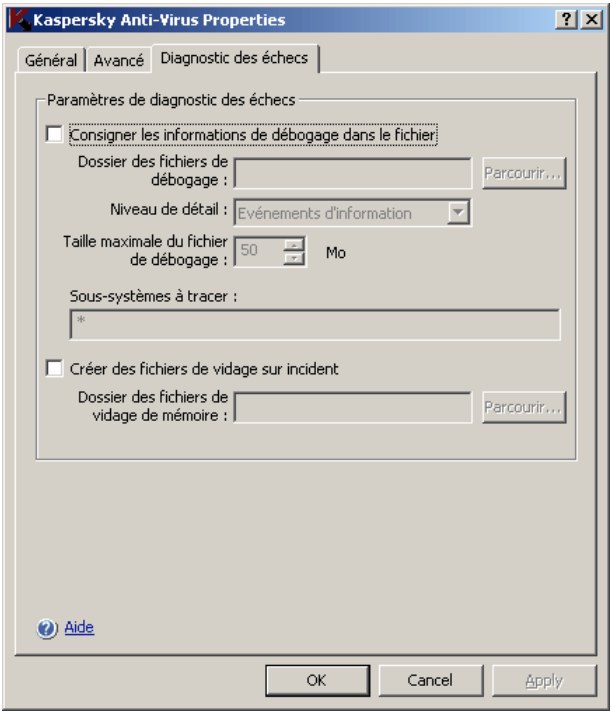

Illustration 8. Boîte de dialogue **Propriétés**, onglet **Diagnostic des échecs**

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

CHAPITRE 4. IMPORTATION ET EXPORTATION DES PARAMETRES DE KASPERSKY ANTI-VIRUS

Le présent chapitre aborde les sujets suivants :

- Présentation de l'importation et de l'exportation des paramètres (cf. point 4.1, p. 50) ;
- Exportation des paramètres (cf. point 4.2, p. 51) ;
- Importation des paramètres (cf. point 4.3, p. 52).

4.1. Présentation de l'importation et de l'exportation des paramètres

Si vous devez attribuer la même valeur à plusieurs paramètres de Kaspersky Ani-Virus sur plusieurs serveurs protégés, vous pouvez configurer Kaspersky Anti-Virus sur un serveur, exporter la configuration au format XML puis importer ce fichier dans les copies de Kaspersky Anti-Virus installées sur les autres serveurs.

Vous pouvez enregistrer tous les paramètres de Kaspersky Anti-Virus ou les paramètres des composants distincts.

En cas d'exportation de tous les paramètres de Kaspersky Anti-Virus, les paramètres généraux de Kaspersky Anti-Virus et les paramètres des composants suivants sont enregistrés dans le fichier :

- Protection en temps réel des fichiers ;
- Analyse des scripts ;
- Interdiction de l'accès des ordinateurs ;
- Analyse à la demande ;

- Mise à jour des bases et des modules de Kaspersky Anti-Virus ;
- Quarantaine ;
- Sauvegarde ;
- Rapports ;
- Notifications ;
- Zone de confiance.

Les privilèges des comptes utilisateur sont également préservés.

Kaspersky Anti-Virus n'exporte pas les paramètres des tâches de groupe, la liste des ordinateurs interdit d'accès et les mots de passe.

Kaspersky Anti-Virus exporte tous les mots de passe qu'il utilise, par exemple les données des comptes pour l'exécution des tâches ou la connexion au serveur proxy, et les conserve dans le fichier de configuration dans une forme cryptée. Ils peuvent être importés uniquement par Kaspersky Anti-Virus sur ce même ordinateur, s'il n'y a pas eu de réinstallation ou de mise à jour. Kaspersky Anti-Virus sur un autre ordinateur ne les importera pas. Après l'importation des paramètres sur un autre ordinateur, vous devrez saisir tous les mots de passe manuellement.

Si une stratégie de Kaspersky Administration Kit est active au moment de l'exportation des paramètres, alors Kaspersky Anti-Virus exporte non pas les valeurs appliquées par la stratégie mais celles en vigueur avant son application.

Remarque

Les paramètres importés ne sont pas appliqués aux tâches en exécution. Ils sont appliqués uniquement au lancement suivant. Il est conseillé d'interrompre les tâches des composants avant d'importer les paramètres.

4.2. Exportation des paramètres

Pour exporter les paramètres dans un fichier de configuration :

1. Si vous avez modifié les paramètres dans la console de Kaspersky Anti-Virus, avant d'exporter les paramètres, cliquez sur le bouton **Enregistrer** afin d'enregistrer les nouvelles valeurs.
2. Exécutez une des actions suivantes :
   - Pour exporter tous les paramètres de Kaspersky Anti-Virus, ouvrez le menu contextuel du nom du composant enfichable Kaspersky Anti-Virus dans la fenêtre de la console et sélectionnez la commande **Exporter les paramètres** ;

- Pour exporter les paramètres d'un composant individuel, ouvrez le menu contextuel du nœud correspond à cette fonction dans l'arborescence de la console et sélectionnez la commande **Exporter les paramètres**.

La fenêtre de bienvenue de l'Assistant d'exportation des paramètres s'ouvre.

3. Suivez les instructions affichées dans les fenêtres de l'Assistant : indiquez le nom du fichier de configuration dans lequel vous souhaitez enregistrer les paramètres ainsi que le chemin d'accès à celui-ci.

> **Remarque**
>
> Si une stratégie de Kaspersky Administration Kit est active au moment de l'exportation des paramètres, alors Kaspersky Anti-Virus exporte non pas les valeurs appliquées par la stratégie mais celles en vigueur avant son application.

4. Dans la fenêtre **Fin de l'exportation**, cliquez sur **OK** pour fermer l'Assistant d'exportation des paramètres.

4.3. Importations des paramètres

Pour importer les paramètres du fichier de configuration :

1. Exécutez une des actions suivantes :

   - Pour importer tous les paramètres de Kaspersky Anti-Virus, ouvrez le menu contextuel du nom du composant enfichable Kaspersky Anti-Virus dans l'arborescence de la console et sélectionnez la commande **Importer les paramètres** ;
   - Pour importer les paramètres d'un composant individuel, ouvrez le menu contextuel du noeud correspond à cette fonction dans l'arborescence de la console et sélectionnez la commande **Importer les paramètres**.

   La fenêtre de bienvenue de l'Assistant d'importation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : identifiez le fichier de configuration que vous souhaitez importer.

Remarque

Une fois que les paramètres de Kaspersky Anti-Virus et de ses composants auront été importés, vous ne pourrez plus revenir à leurs valeurs antérieures.

3. Dans la fenêtre **Fin de l'importation** cliquez sur le bouton **OK** afin de fermer l'Assistant d'importation des paramètres.
4. Dans la console de Kaspersky Anti-Virus, dans le panneau des instruments, cliquez sur le bouton **Actualiser**  afin d'afficher les paramètres importés.

Remarque

Kaspersky Anti-Virus n'importe pas les mots de passe (les données des comptes utilisateur pour l'exécution de tâches ou la connexion au serveur proxy) d'un fichier créé sur un autre ordinateur ou sur ce même ordinateur après une réinstallation ou de mise à jour de Kaspersky Anti-Virus. Après la fin de l'importation, vous devrez saisir les mots de passe manuellement.

CHAPITRE 5. ADMINISTRATION DES TACHES

Le présent chapitre aborde les sujets suivants :

- Catégorie de tâches de Kaspersky Anti-Virus en fonction de leur création et de leur exécution (cf. point 5.1, p. 54) ;
- Création de tâches (cf. point 5.2, p. 56) ;
- Enregistrement d'une tâche après la modification de ses paramètres (cf. point 5.3, p. 58) ;
- Changement de nom d'une tâche (cf. point 5.4, p. 59) ;
- Suppression d'une tâche (cf. point 5.5, p. 59) ;
- Lancement / suspension / rétablissement / arrêt manuel d'une tâche (cf. point 5.6, p. 60) ;
- Programmation des tâches (cf. point 5.7, p. 60) ;
- Consultation des statistiques de la tâche (cf. point 5.8, p. 64) ;
- Lancement de la tâche sous un autre compte utilisateur (cf. point 5.9, p. 65).

5.1. Catégories de tâches dans Kaspersky Anti-Virus

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

Les tâches sont réparties entre les tâches *locales* et les tâches *de groupe*. Les tâches locales peuvent être p*rédéfinies* ou *définies par l'utilisateur*.

Tâches locales

Les tâches locales sont uniquement exécutées sur le serveur protégé pour lequel elles ont été créées.

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

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

Tâches de groupe

Les tâches globales et les tâches de groupe, créées dans la console d'administration de Kaspersky Administration Kit figurent dans la console de Kaspersky Anti-Virus dans MMC. Elles sont toutes désignées comme des tâches de groupe dans la console de Kaspersky Anti-Virus. Vous pouvez administrer les tâches de groupe et les configurer au départ de Kaspersky Administration Kit. La console de Kaspersky Anti-Virus dans MMC vous permet également de consulter l'état des tâches de groupe.

La console de Kaspersky Anti-Virus affiche les informations relatives aux tâches (cf. exemple dans l'illustration 9).

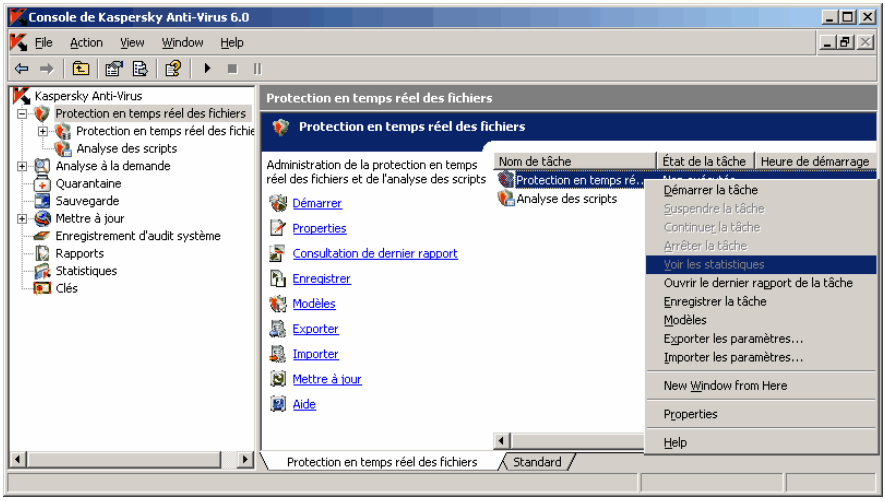

Illustration 9. Tâches de protection en temps réel dans la fenêtre de la console de Kaspersky Anti-Virus.

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

Les opérations d'administration des tâches sont consignées dans le journal d'audit système (cf. point 13.3, p. 219).

5.2. Nouvelle tâche

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

Afin de créer une nouvelle tâche d'analyse à la demande :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Analyse à la demande** et sélectionnez la commande **Ajouter tâche** (cf. ill. 10).

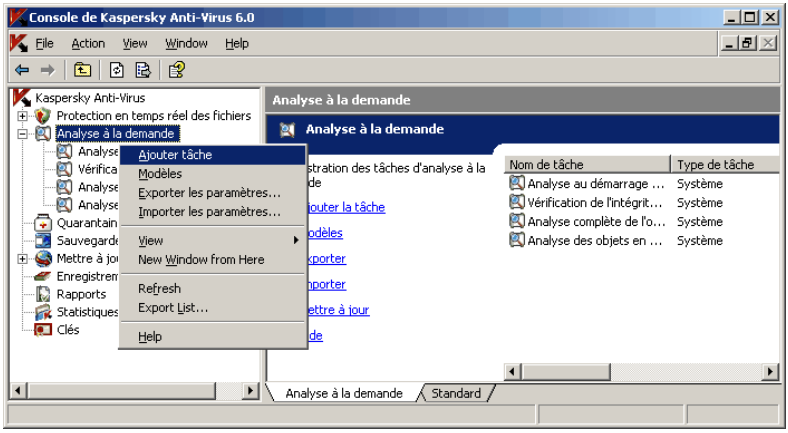

Illustration 10. Exemple de création d'une tâche

La boîte de dialogue **Nouvelle tâche** s'ouvre (cf. ill. 11).

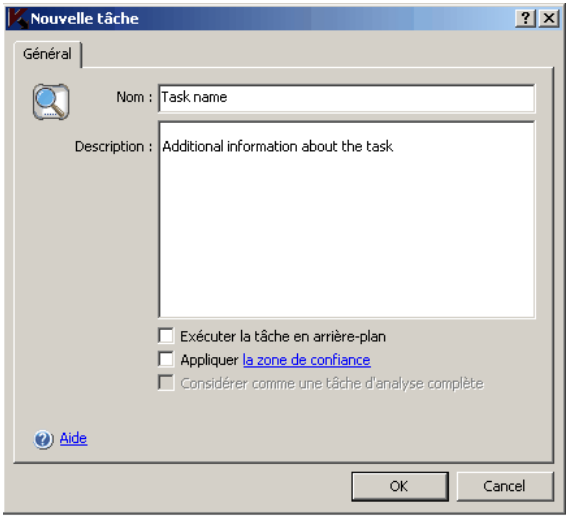

Illustration 11. Boîte de dialogue **Nouvelle tâche**

2. Saisissez les informations suivantes relatives à la tâche :
   - **Nom** : nom de la tâche, 100 caractères maximum ;

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

3. Si la tâche doit être exécutée dans un processus à faible priorité, cochez la case **Exécuter la tâche en arrière-plan** (pour en savoir plus sur les priorités des tâches de Kaspersky Anti-Virus, lisez le point 9.3, p. 145).
4. Cliquez sur **OK**. La tâche est créée. Une ligne reprenant les informations qui la concernent apparaît dans la fenêtre de la console.

5.3. Enregistrement d'une tâche après modification de ses paramètres

Vous pouvez modifier les paramètres d'une tâche en cours d'exécution ou arrêtée (suspendue) :

- *En cas de modification des paramètres d'une tâche en cours d'exécution* : dans les tâches de protection en temps réel, les nouvelles valeurs des paramètres seront appliquées directement après leur enregistrement ; dans les autres tâches, ces valeurs entrent en vigueur au prochain lancement de la tâche ;
- *En cas de modification des paramètres d'une tâche arrêtée* : les nouvelles valeurs des paramètres seront appliquées une fois qu'elles auront été enregistrées et que la tâche aura été lancée.

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

Remarque

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

Pour savoir comment configurer les paramètres de la tâche **Protection en temps réel des fichiers**, lisez le point 6.2 à la page 69.

Pour savoir comment configurer les paramètres d'une tâche d'analyse à la demande, lisez le point 9.2 à la page 122.

La configuration des paramètres des tâches de mise à jour est décrite au point 10.5 à la page 160.

5.4. Renommer

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

Afin de renommer une tâche :

1. Ouvrez le menu contextuel de la tâche et sélectionnez **Propriétés**.
2. Dans la boîte de dialogue **Propriétés**, saisissez le nouveau nom de la tâche dans le champ **Nom**, puis cliquez sur **OK**.

La tâche sera ainsi renommée. L'opération sera consignée dans le journal d'audit système (cf. point 13.3, p. 219).

Pour en savoir plus sur la programmation des tâches, consultez le point 5.7 à la page 60.

5.5. Suppression d'une tâche

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

Pour supprimer une tâche :

1. Ouvrez le menu contextuel de la tâche et sélectionnez **Supprimer**.
2. Dans la boîte de dialogue **Supprimer tâche**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

La tâche sera supprimée et cette opération sera consignée dans le journal d'audit système (cf. point 13.3, p. 219).

5.6. Lancement / suspension / rétablissement / arrêt manuel d'une tâche

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

Pour lancer / suspendre / reprendre / arrêter une tâche, ouvrez le menu contextuel de la tâche et sélectionnez la commande requise : ***Lancer****,* ***Suspendre****,* ***Reprendre*** *ou* ***Arrêter****.*

L'opération sera exécutée. L'état de la tâche dans le panneau des résultats changera ; cette opération sera consignée dans le journal d'audit système (cf. point 13.3, p. 219).

Remarque

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

5.7. Programmation des tâches

Cette section aborde les sujets suivants :

- Programmation d'une tâche(cf. point 5.7.1, p. 60).
- Activation / désactivation d'une tâche programmée (cf. point 5.7.2, p. 64).

Les paramètres de la programmation sont décrits au point B.2 à la page 391.

5.7.1. Programmation d'une tâche

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

Une description des paramètres de programmation est proposée au point B.2 à la page 391.

Pour programmer l'exécution d'une tâche :

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez programmer l'exécution et sélectionnez **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de la tâche** (cf. ill. 12), activez le lancement programmé des tâches sur l'onglet **Planification** : cochez la case **Exécuter de manière planifiée**.

> **Remarque**
>
> Les champs avec les paramètres de programmation de la tâche prédéfinie ne sont pas disponibles si le lancement programmé de cette tâche prédéfinie est interdit par une stratégie de l'application Kaspersky Administration Kit (cf. point 19.4, p. 299).

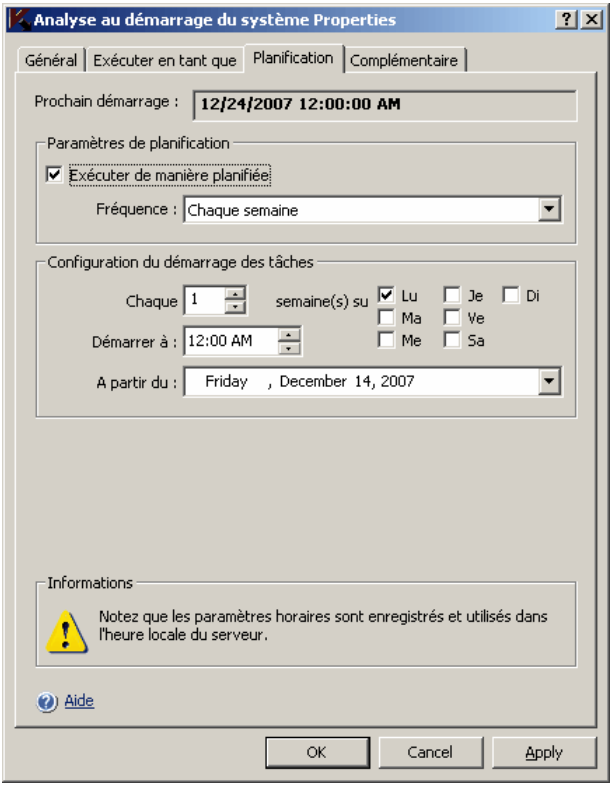

Illustration 12. Exemple de l'onglet **Planification** avec la valeur **Fréquence : Chaque semaine**

3. Configurez l'horaire en fonction de vos besoins.

   a) Précisez la fréquence d'exécution de la tâche (cf. point B.2.1, p. 392) : choisissez une des options suivantes dans la liste **Fréquence** : **Chaque heure**, **Chaque jour**, **Chaque semaine**, **Au lancement de Kaspersky Anti-Virus**, **A l'actualisation des bases** :

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

   b) Dans le champ **Démarrer à**, indiquez l'heure de la première exécution de la tâche.

   c) Dans le champ **A partir du**, indiquez la date d'entrée en vigueur de la planification (cf. point B.2.2, p. 393).

   Remarque

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

   La valeur **Lancement de la tâche interdit par la stratégie** dans le champ **Prochain démarrage** apparaît si les paramètres de la stratégie actuelle de Kaspersky Administration Kit interdisent l'exécution des tâches programmées prédéfinies (pour de plus amples informations, consultez le point 19.4 à la page 299).

4. Sur l'onglet **Complémentaire** (cf. ill. 13), configurez les autres paramètres en fonction de vos besoins.

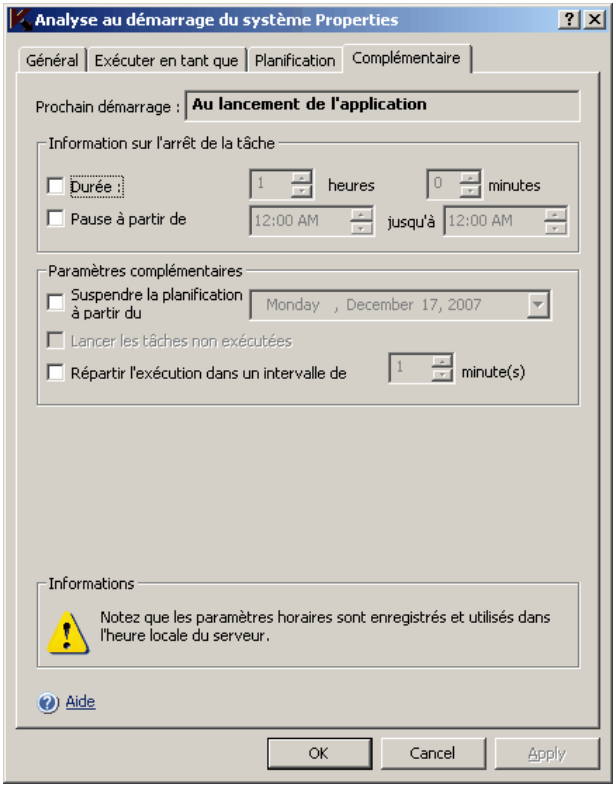

Illustration 13. Boîte de dialogue **Propriétés de la tâche**, onglet **Complémentaire**

a) Pour définir la durée maximale d'exécution d'une tâche, dans le champ **Durée** du groupe **Information sur l'arrêt de la tâche**, saisissez les heures et les minutes souhaitées (cf. point B.2.4, p. 395).

b) Pour définir la plage horaire de la journée au cours de laquelle l'exécution de la tâche sera suspendue, saisissez les heures de début et de fin dans le champ **Pause à partir de... jusqu'à** du groupe **Information sur l'arrêt de la tâche** (cf. point B.2.5, p. 396).

c) Pour définir la date à partir de laquelle la programmation ne sera plus active, cochez la case **Suspendre la planification à partir du** et à l'aide de la boîte de dialogue **Calendrier**, sélectionnez la date à partir de laquelle la planification ne sera plus en vigueur (cf. point B.2.3, p. 394).

d) Pour activer l'exécution des tâches non exécutées, cochez la case **Lancer les tâches non exécutées** (cf. point B.2.6, p. 396).

e) Pour activer l'utilisation du paramètre **Répartition des lancements dans l'intervalle**, cochez la case **Répartir l'exécution dans un intervalle de** et définissez la valeur du paramètre en minutes (cf. point B.2.7, p. 397).

5. Cliquez sur **OK** afin d'enregistrer les modifications introduites dans la boîte de dialogue **Propriétés de la tâche**.

5.7.2. Activation et désactivation de l'exécution programmée

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

Pour activer une désactiver une programmation :

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez activer ou désactiver la programmation et sélectionnez la commande **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de la tâche : Planification** exécutez une des actions suivantes :
   - Pour activer la planification, cochez la case **Exécuter de manière planifiée** ;
   - Pour désactiver la planification, désélectionnez la case **Exécuter de manière planifiée**.
3. Cliquez sur **OK**.

5.8. Consultation des statistiques des tâches

Tandis que la tâche est exécutée, vous pouvez consulter en temps réel les informations détaillées relatives à son exécution depuis le début jusqu'à maintenant dans la boîte de dialogue **Statistiques**.

Les informations de la boîte de dialogue **Statistiques** sont accessibles lorsque la tâche est suspendue. Après la fin ou la suspension de la tâche, vous pouvez

consulter ces informations dans le rapport détaillé sur les événements survenus dans la tâche (cf. point 13.2.4, p. 211).

Pour consulter les statistiques d'une tâche, ouvrez le menu contextuel de la tâche qui vous intéresse dans la fenêtre de la console et sélectionnez la commande ***Voir les statistiques****.*

5.9. Utilisation des comptes utilisateur pour l'exécution des tâches

Cette section aborde les sujets suivants :

- Présentation de l'utilisation de comptes utilisateur pour l'exécution de tâches (cf. point 5.9.1, p. 65) ;
- Définition du compte utilisateur pour l'exécution de la tâche (cf. point 5.9.2, p. 66).

5.9.1. Présentation de l'utilisation des comptes utilisateur pour l'exécution des tâches

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

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

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

- Pour la tâche de mise à jour, si la source de mise à jour est un répertoire de réseau partagé sur un autre ordinateur du réseau ;
- Pour la mise à jour, si l'accès à la source des mises à jour s'opère via un serveur proxy doté de la vérification intégrée de l'authenticité Microsoft Windows (authentification NTLM) ;

- Dans les tâches d'analyse à la demande, si le compte **Système local** (**SYSTEM**) ne jouit pas des privilèges d'accès à un des objets à analyser (par exemple, aux fichiers d'un répertoire partagé sur le réseau).

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

5.9.2. Définition du compte utilisateur pour l'exécution de la tâche

Pour définir le compte à utiliser pour l'exécution d'une tâche :

1. Ouvrez le menu contextuel de la tâche et sélectionnez la commande **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de la tâche**, ouvrez l'onglet **Exécuter en tant que** (cf. ill. 14).

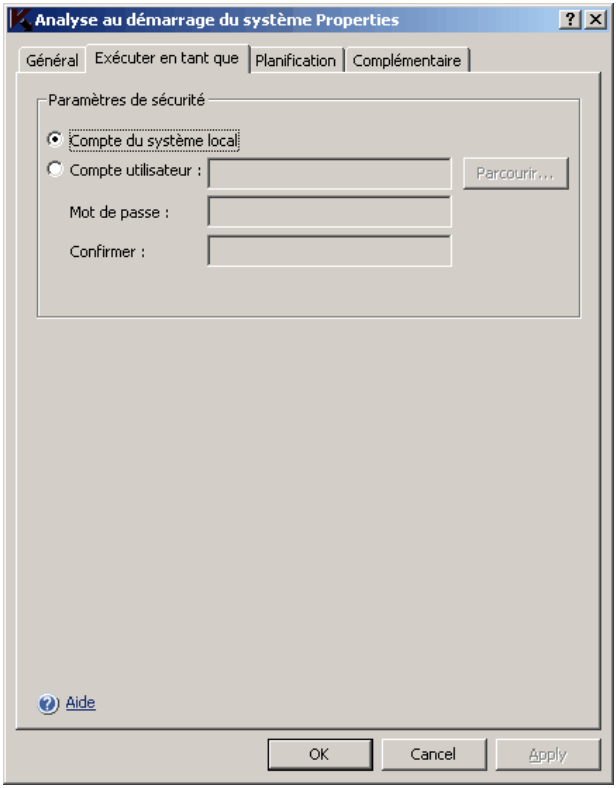

Illustration 14. Boîte de dialogue **Propriétés de la tâche**, onglet **Exécuter en tant que**

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

   a) Sélectionnez **Compte utilisateur**.

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

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

   c) Cliquez sur **OK**.

CHAPITRE 6. PROTECTION EN TEMPS REEL DES FICHIERS

Le présent chapitre aborde les sujets suivants :

- Présentation des tâches de protection en temps réel (cf. point 6.1, p. 68) ;
- Configuration de la tâche **Protection en temps réel des fichiers** (cf. point 6.2, p. 69) ;
- Statistiques de la tâche **Protection en temps réel des fichiers** (cf. point 6.2.3, p. 91) ;
- Configuration de la tâche **Analyse des scripts** : sélection des actions à exécuter sur les scripts suspects (cf. point 6.4, page 94) ;
- Statistiques de la tâche **Analyse des scripts** (cf. point 6.5, p. 95).

6.1. Présentation des tâches de la protection en temps réel

Kaspersky Anti-Virus prévoit deux tâches prédéfinies de protection en temps réel : **Protection en temps réel des fichiers** et **Analyse des scripts**. Pour obtenir de plus amples informations sur la fonction *Protection en temps réel*, lisez le point 1.1.1 à la page 15.

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

Vous pouvez configurer la tâche **Protection en temps réel des fichiers** : créer des couvertures d'analyse et définir des paramètres de sécurité pour les nœuds sélectionnés, configurer l'interdiction de l'accès des ordinateurs, appliquer une zone de confiance (cf. point 6.2, p. 69).

Quand la tâche **Analyse des scripts** est exécutée, Kaspersky Anti-Virus interdit l'exécution des scripts qu'il juge dangereux. Si Kaspersky Anti-Virus juge un script suspect, il exécute l'action sélectionnée : interdiction ou autorisation de

l'exécution. Pour savoir comment autoriser ou interdire l'exécution des scripts suspects, consultez le point 6.4 à la page 94.

6.2. Configuration de la tâche *Protection en temps réel des fichiers*

Par défaut, la tâche prédéfinie **Protection en temps réel des fichiers** possède les paramètres décrits au tableau 2. Vous pouvez modifier les valeurs de ces paramètres et configurer ainsi la tâche.

Tableau 2. Paramètres par défaut de la tâche **Protection en temps réel des fichiers**

Paramètre	Valeur par défaut	Description
Couverture de protection	Tout le serveur	Vous pouvez limiter la couverture de protection (cf. point 6.2.1, p. 72).
Paramètres de sécurité	Identiques pour toutes les couvertures de protection ; correspondent au niveau de protection **Recommandé**.	Pour les nœuds sélectionnés dans l'arborescence des ressources fichier du serveur, vous pouvez : • Appliquer un autre niveau de protection prédéfini (cf. point 6.2.2.1, p. 79) ; • Modifier les paramètres de protection (cf. point 6.2.2.2, p. 82). Vous pouvez enregistrer les paramètres de protection du noeud sélectionné dans un modèle afin de pouvoir l'appliquer par la suite à n'importe quel autre noeud (cf. point 6.2.2.3, p. 86).

Paramètre	Valeur par défaut	Description
Mode de protection des objets	A l'accès et à la modification	Vous pouvez sélectionner le mode de protection des objets, à savoir dans quel type d'accès aux objets Kaspersky Anti-virus les analyse-t-il. Pour savoir comment choisir le mode de protection des objets, lisez le point 6.2.3 à la page 90. Pour en savoir plus sur les modes de protection des objets, lisez le point B.3.1 à la page. 399.
Interdiction de l'accès des ordinateurs	Désactivé	Vous pouvez interdire l'accès des ordinateurs au serveur protégé en cas de tentative d'écriture sur le serveur d'objets infectés ou suspects (cf. Chapitre 7, p. 97).
Zone de confiance	Appliquée Les programmes d'administration à distance **RemoteAdmin** sont exclus ainsi que les fichiers recommandés par Microsoft Corporation si, au moment de l'installation de Kaspersky Anti-Virus, vous avez sélectionné **Ajouter les menaces selon le masque not-a-virus:RemoteAdmin* aux exclusions** et **Ajouter les fichiers recommandés par Microsoft aux exclusions**.	Une liste unique d'exclusions que vous pouvez appliquer dans des tâches d'analyse à la demande sélectionnée et dans la tâche de **Protection en temps réel des fichiers**. Chapitre 8 à la page 109 contient des informations sur la création et l'application de la zone de confiance.

*Pour configurer la tâche **Protection en temps réel des fichiers** :*

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Sélectionnez le noeud **Protection en temps réel des fichiers**.

Le panneau des résultats affiche l'arborescence des ressources fichiers du serveur et la boîte de dialogue **Niveau de sécurité** (mode standard) (cf. ill. 15).

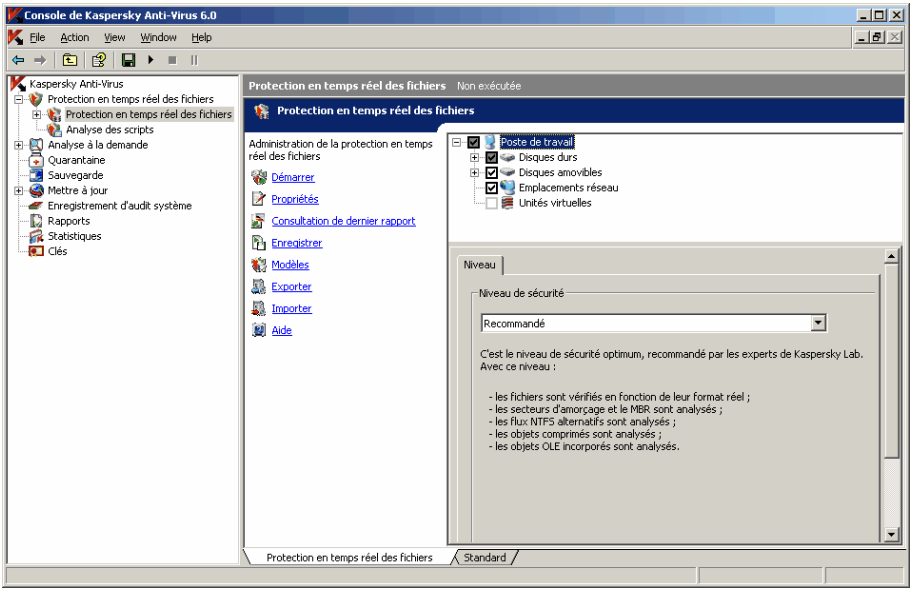

Illustration 15. Tâche **Protection en temps réel des fichiers** ouverte

3. Le cas échéant, configurez les paramètres de la tâche.
4. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

Pour savoir comment :

- Exécution / suspension / reprise / arrêt manuel d'une tâche, cf. point 5.6, p. 60.
- Lancer une tâche programmée, cf. point 5.7, p. 60.

6.2.1. Couverture de protection dans la tâche *Protection en temps réel des fichiers*

Cette section aborde les sujets suivants :

- Constitution de la couverture de protection de la tâche *Protection en temps réel des fichiers*) (cf. point 6.2.1.1, p. 72) ;
- Secteurs définis du serveur qui peuvent être repris dans la couverture de protection (cf. point 6.2.1.2, p. 73) ;
- Constitution de la couverture de protection : exclure ou non certains secteurs du serveur (cf. point 6.2.1.3, p. 75) ;
- Couverture de protection virtuelle : disques, répertoires et fichiers qui sont surveillés temporairement sur le serveur ainsi que les répertoires et les fichiers qui sont créés de manière dynamique sur le serveur par divers applications et services (cf. point 6.2.1.4, p. 76) ;
- Création d'une couverture de protection virtuelle (cf. point 6.2.1.5 à la page 77).

6.2.1.1. Présentation de la constitution d'une couverture de protection dans la tâche *Protection en temps réel des fichiers*

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

Dans la console de Kaspersky Anti-Virus, la couverture de protection se présente sur la forme d'une arborescence des ressources fichiers du serveur que Kaspersky Anti-Virus peut analyser.

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

☑ Nœud repris dans la couverture de protection.

☐ Noeud exclu de la couverture de protection.

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

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

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

6.2.1.2. Couvertures de protection prédéfinies

Quand vous ouvrez la tâche **Protection en temps réel des fichiers**, l'arborescence des ressources fichier du serveur s'affiche dans le panneau des résultats (cf. ill. 16).

Remarque

L'arborescence des ressources fichier illustre les nœuds que vous pouvez accéder en lecture en fonction des paramètres de sécurité de Microsoft Windows.

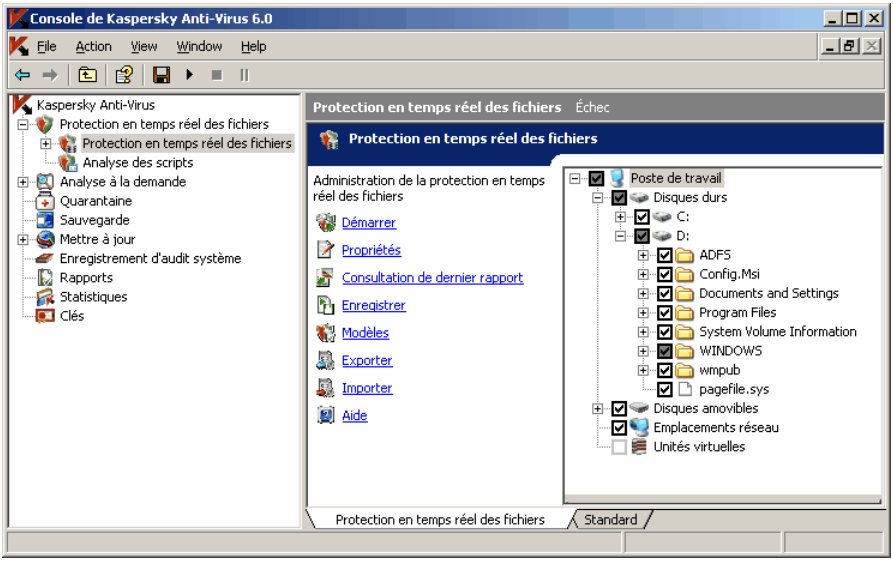

Illustration 16. Exemple d'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus.

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

- **Disques durs**. Kaspersky Anti-Virus analyse les fichiers du disque dur du serveur.
- **Disques amovibles**. Kaspersky Anti-Virus analyse les fichiers sur les disques amovibles tels que les disques compacts ou les clés USB.
- **Emplacements réseau**. Kaspersky Anti-Virus analyse les fichiers enregistrés dans les répertoires réseau ou lus par les applications exécutées sur le serveur. Kaspersky Anti-Virus n'analyse pas les fichiers dans les répertoires de réseau lorsqu'ils sont sollicités par des applications d'autres ordinateurs.
- **Unités virtuelles**. Vous pouvez inclure dans la couverture de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur le serveur, par exemple les disques partagés d'une grappe (créer *couverture de protection virtuelle*).

Remarque

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

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

6.2.1.3. Constitution de la couverture de protection

Pour composer la couverture de protection :

1. Ouvrez la tâche **Protection en temps réel des fichiers**.
2. Dans le panneau des résultats, exécutez les actions suivantes dans les ressources fichier du serveur :
   - Pour exclure un noeud particulier de la couverture de protection, déployez l'arborescence des ressources de fichiers pour afficher le noeud requis et désélectionnez la case en regard de son nom.
   - Pour sélectionner uniquement les nœuds que vous souhaitez inclure dans la couverture d'analyse, désélectionnez la case **Poste de travail** puis :
     - Si vous souhaitez inclure tous les disques d'un même type, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**) ;
     - Si vous souhaitez inclure un disque particulier du type requis, déployez le noeud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque. Par exemple, pour sélectionner le disque amovible **F:**, ouvrez le noeud **Disques amovibles** et cochez la case en regard du disque **F:** ;
     - Si vous souhaitez inclure uniquement un répertoire particulier du disque, déployez l'arborescence des ressources du serveur afin d'afficher le répertoire que vous souhaitez inclure dans la

couverture d'analyse puis, cochez la case en regard de son nom. Vous pouvez inclure des fichiers de la même manière.

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

Remarque

Vous pouvez exécuter la tâche **Protection en temps réel des fichiers** uniquement si au moins un noeud de l'arborescence des ressources fichier du serveur figure dans la couverture de protection.

Remarque

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

6.2.1.4. Couverture de protection virtuelle

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

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

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

Pour savoir comment créer une couverture de protection virtuelle dans la tâche **Protection en temps réel des fichiers**, consultez le point 6.2.1.5 à la page 77.

Pour savoir comment créer une couverture de protection virtuelle dans les tâches d'analyse à la demande, consultez le point 9.2.1.5 à la page 129.

6.2.1.5. Création d'une couverture de protection virtuelle : inclusion des disques, répertoires et fichiers dynamiques dans la couverture de protection

Pour ajouter un disque virtuel à la couverture de protection :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** et sélectionnez le noeud subalterne **Protection en temps réel des fichiers**.
2. Dans l'arborescence des ressources fichier du serveur du panneau des résultats, ouvrez le menu contextuel du noeud **Unités virtuelles** et dans la liste des noms disponibles, sélectionnez le nom du disque virtuel créé (cf. ill. 17).

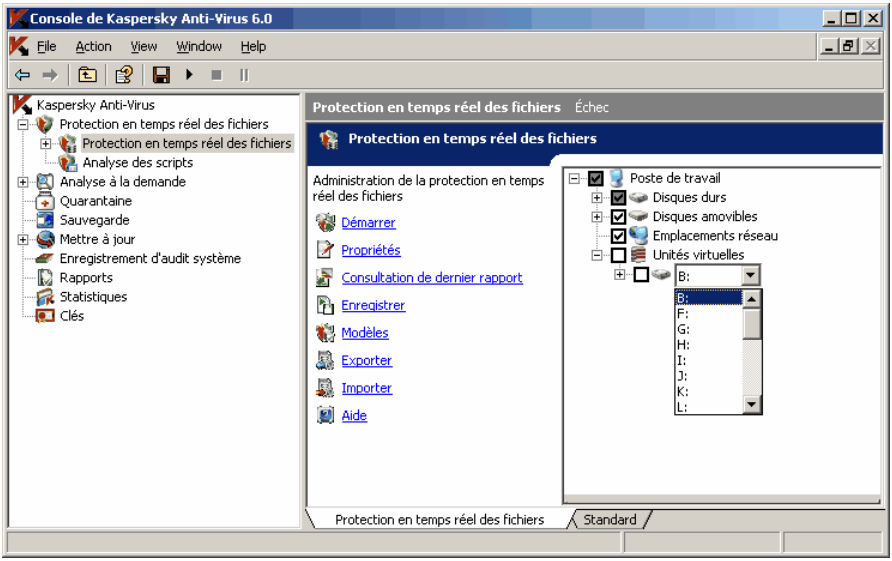

Illustration 17. Sélection du nom d'unité virtuelle créé

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

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

Pour ajouter un répertoire ou un fichier virtuel dans la couverture de protection :

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

2. Accédez au panneau des résultats et dans l'arborescence des ressources fichiers du serveur ouvrez le menu contextuel du noeud auquel vous souhaitez ajouter un répertoire ou un fichier et sélectionnez **Ajouter un dossier virtuel** ou **Ajouter un fichier virtuel**.

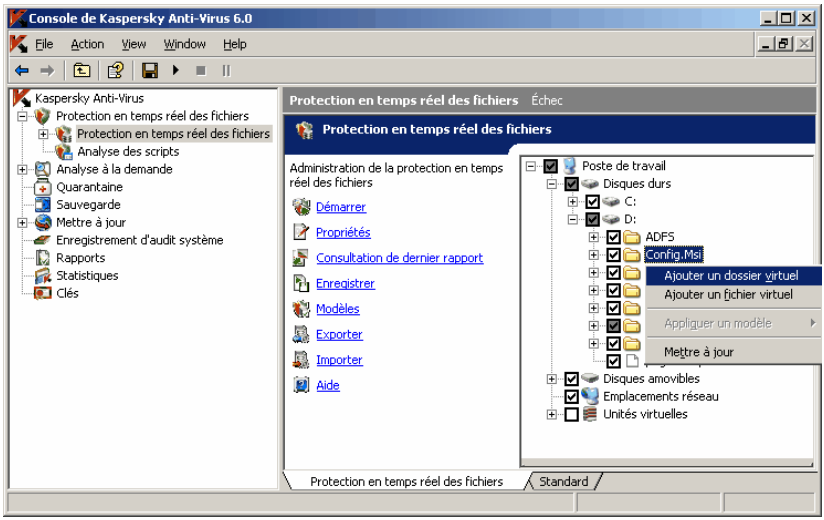

Illustration 18. Ajout d'un fichier virtuel

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

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

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

6.2.2. Configuration des paramètres de sécurité du noeud sélectionné

Vous pouvez configurer les paramètres de protection du noeud sélectionné dans l'arborescence des ressources fichier du serveur de la manière suivante :

- Sélectionnez un des trois niveaux de protection prédéfinis (vitesse maximale, recommandé ou protection maximum) (cf. point 6.2.2.1, p. 79) ;
- Modifier manuellement les paramètres de protection du noeud sélectionné (cf. point 6.2.2.2, p. 82).

Vous pouvez enregistrer les paramètres de protection du noeud sélectionné dans un modèle afin de pouvoir l'appliquer par la suite à n'importe quel autre noeud (cf. point 6.2.2.3, p. 86).

6.2.2.1. Sélection des niveaux prédéfinis de protection dans la tâche *Protection en temps réel des fichiers*

Pour les nœuds sélectionnés dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des niveaux prédéfinis de protection suivant : a) vitesse maximale, b) recommandé ou c) protection maximum. Chacun de ces niveaux possède sa propre sélection de paramètres de sécurité. Les valeurs des paramètres des niveaux prédéfinis sont reprises au tableau 3 à la page 80.

Vitesse maximale

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

Recommandé

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

Protection maximum

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

Tableau 3. Niveaux de protection prédéfinis et valeurs des paramètres correspondants

Paramètres	Niveau de sécurité		
	Vitesse maximale	**Recommandé**	**Protection maximum**
Objets à analyser (cf. point B.3.2, p. 400)	Selon l'extension	En fonction du format	En fonction du format
Analyse uniquement des objets neufs et modifiés (cf. point B.3.3, p. 402)	Activé	Activé	Activé
Actions à exécuter sur les objets infectés (cf. point B.3.5, p. 404)	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. point B.3.6, p. 406)	Quarantaine	Quarantaine	Quarantaine
Exclusion des objets(cf. point B.3.8, p. 410)	Non	Non	Non
Exclusion des menaces (cf. point B.3.9, p. 411)	Non	Non	Non
Durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413)	60 s	60 s	60 s
Taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413)	8 Mo	8 Mo	Non installé
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. point B.3.2, p. 400)	Oui	Oui	Oui

Paramètres	Niveau de sécurité		
	Vitesse maximale	**Recommandé**	**Protection maximum**
Analyse des secteurs d'amorçage (cf. point B.3.2, p. 400)	Oui	Oui	Oui
Traiter les objets composés (cf. point B.3.4, p. 402)	Objets compactés* * Uniquement si neufs ou modifiés	• Archives SFX • Objets compactés* ; • Objets OLE intégrés* * Uniquement les archives nouvelles	• Archives SFX* ; • Objets compactés* ; • Objets OLE intégrés* * Tous les objets

Remarque

N'oubliez pas que les paramètres de sécurité **Mode de protection**, **Application de la technologie iChecker** et **Application de la technologie iSwift** ne figurent pas parmi les paramètres des niveaux prédéfinis. Ils sont activés par défaut. Si, après avoir choisi un des niveaux de protection prédéfinis, vous modifiez la valeur des paramètres **Mode de protection**, **Application de la technologie iChecker** ou **Application de la technologie iSwift**, le niveau de protection que vous avez défini sera conservé.

Pour sélectionner un des niveaux de protection prédéfinis :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** et sélectionnez le noeud subalterne **Protection en temps réel des fichiers**.
2. Accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le noeud auquel vous souhaitez appliquer un des niveaux de protection prédéfini.
3. Assurez-vous que ce noeud est repris dans la couverture de protection (cf. point 6.2.1.3 à la page 75).

4. Dans la boîte de dialogue **Niveau** (cf. ill. 19), sélectionnez le niveau de protection que vous souhaitez appliquer dans la liste **Niveau de sécurité**.

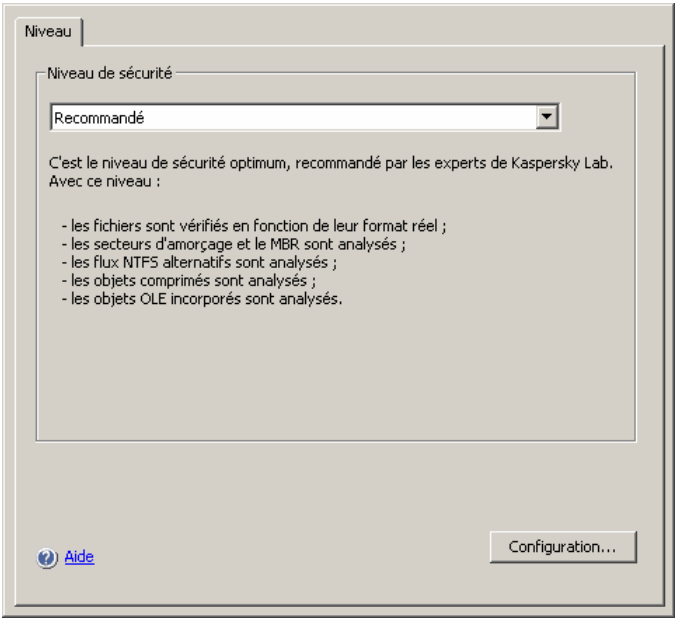

Illustration 19. Boîte de dialogue **Niveau**

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

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

6.2.2.2. Configuration manuelle des paramètres de sécurité

Par défaut, la tâche **Protection en temps réel des fichiers** applique les même paramètres de sécurité à toutes les couvertures de protection. Les valeurs correspondent à celles du niveau prédéfini **Recommandé**. Les valeurs des paramètres de sécurité définis par défaut sont reprises au point 6.2.2.1, p. 79.

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

Les paramètres de sécurité que vous définissez pour un noeud sélectionné seront automatiquement appliqué à tous les nœuds qu'il renferme. Toutefois, si vous attribuez des valeurs distinctes aux paramètres de sécurité du noeud enfant, alors les paramètres de protection du noeud parent ne seront pas appliqués.

Pour configurer manuellement les paramètres de sécurité du noeud sélectionné :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** et sélectionnez le noeud subalterne **Protection en temps réel des fichiers**.
2. Accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le noeud dont vous souhaitez configurer les paramètres de sécurité.
3. Cliquez sur le bouton **Paramètres** dans la partie inférieure de la boîte de dialogue.

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

   Remarque

   Pour savoir comment appliquer le modèle des paramètres de sécurité pour le noeud, consultez le point 6.2.2.3 à la page 86.

4. Configurez les paramètres de sécurité requis pour le noeud sélectionné en fonction de vos exigences :
   - Réalisez les actions suivantes sur l'onglet **Général** (cf. ill. 20) :
     - Sous le titre **Étendue de la protection**, indiquez si Kaspersky Anti-Virus analysera tous les objets de la couverture de protection ou uniquement les objets d'un format ou d'une extension déterminé, si Kaspersky Anti-Virus analysera les secteurs d'amorçage des disques et l'enregistrement principal d'amorçage ou les flux NTFS alternatifs (cf. point B.3.2, p. 400) ;
     - Sous le titre **Optimisation**, indiquez si Kaspersky Anti-Virus analysera tous les objets dans le secteur sélectionné ou seulement les objets neufs ou modifiés (cf. point B.3.3, p. 402) ;
     - Sous le titre **Traiter les objets composés**, précisez les types d'objets composés qui seront analysés par Kaspersky Anti-Virus (cf. point B.3.4, p. 402).

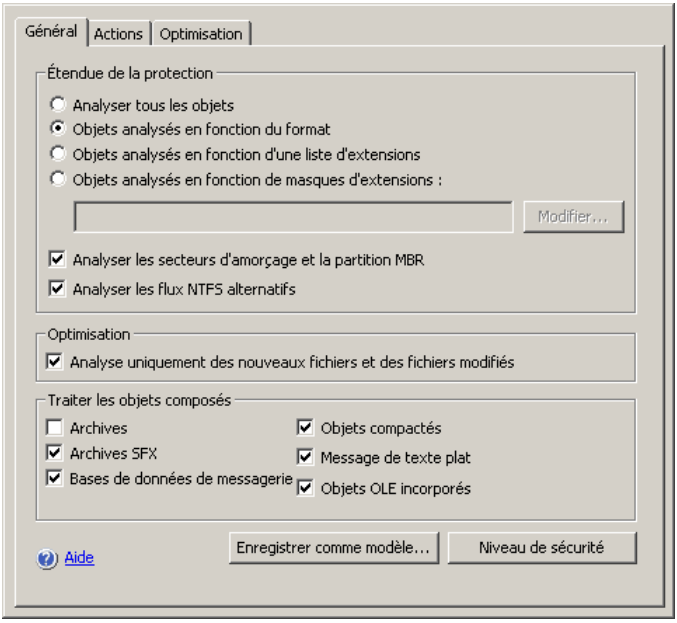

Illustration 20. Boîte de dialogue **Paramètres de sécurité**, onglet **Général**

- Réalisez les actions suivantes sur l'onglet **Actions** (cf. ill. 21) :
  - Sélectionnez l'action à exécuter sur les objets infectés (cf. point B.3.5, p. 404) ;
  - Sélectionnez l'action à exécuter sur les objets suspects (cf. point B.3.6, page 406) ;
  - Le cas échéant, configurez les actions à exécuter sur les objets en fonction du type de menace découverte dans ceux-ci (cf. point B.3.7, p. 408).

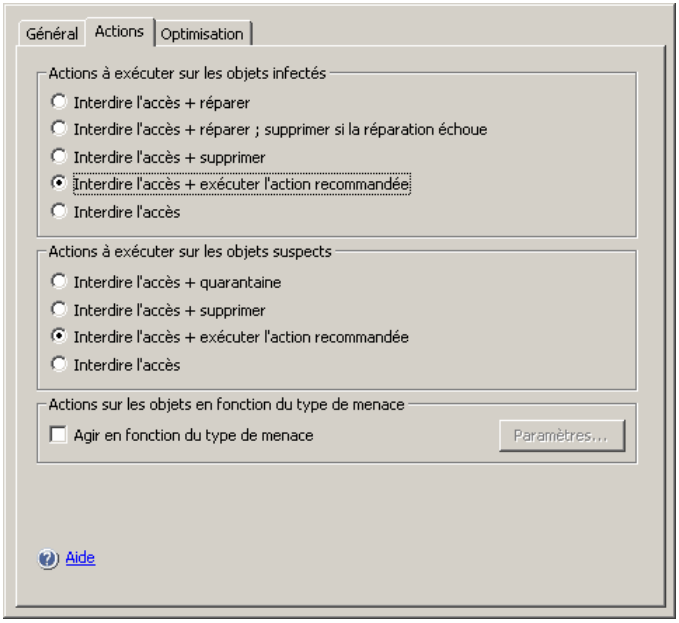

Illustration 21. Boîte de dialogue **Paramètres de sécurité**, onglet **Actions**

- Réalisez les actions suivantes sur l'onglet **Optimisation** (cf. ill. 22), le cas échéant :
  - Excluez des fichiers du traitement selon le nom ou le masque (cf. point B.3.8, p. 410) ;
  - Excluez des menaces du traitement selon le nom ou le masque (cf. point B.3.9, p. 411) ;
  - Indiquez la durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413) ;
  - Indiquez la taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413) ;
  - Activez ou désactivez l'application de la technologie iChecker (cf. point B.3.12, p. 414) ;
  - Activez ou désactivez l'application de la technologie iSwift (cf. point B.3.13, p. 415).

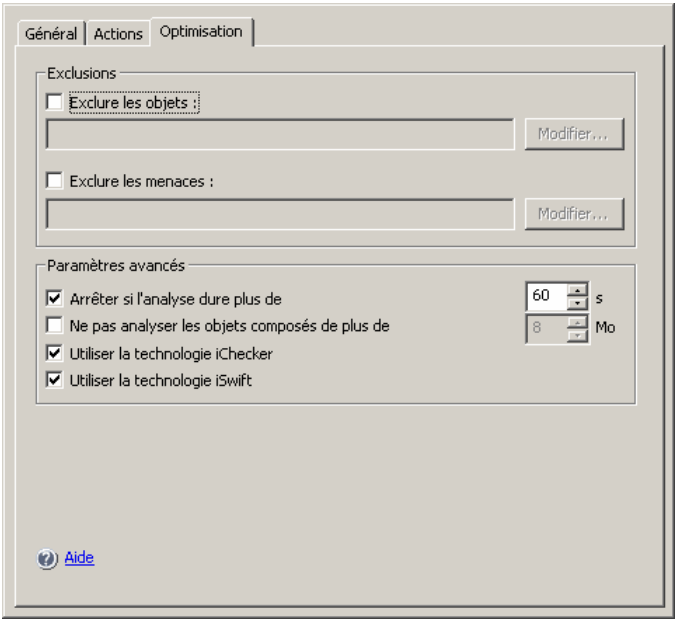

Illustration 22. Boîte de dialogue **Paramètres de sécurité**, onglet **Optimisation**

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

6.2.2.3. Utilisation de modèles dans la tâche *Protection en temps réel des fichiers*

Cette section aborde les sujets suivants :

- Enregistrement de la sélection des paramètres de sécurité dans un modèle (cf. point 6.2.2.3.1, p. 87) ;
- Consultation des paramètres de sécurité dans le modèle (cf. point 6.2.2.3.2, p. 88) ;
- Application du modèle (cf. point 6.2.2.3.3, p. 89) ;
- Suppression du modèle (cf. point 6.2.2.3.4, p. 90).

6.2.2.3.1. Enregistrement des valeurs des paramètres de sécurité dans un modèle

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

Pour enregistrer l'ensemble des valeurs des paramètres de sécurité dans un modèle :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** et sélectionnez le noeud subalterne **Protection en temps réel des fichiers**.
2. Accédez au panneau des résultats et, dans l'arborescence des ressources fichier du réseau, sélectionnez le noeud dont vous souhaitez enregistrer les paramètres de sécurité.
3. Cliquez sur le bouton **Paramètres** dans la partie inférieure de la boîte de dialogue.
4. Dans la boîte de dialogue **Paramètres de la couverture de protection**, onglet **Général**, cliquez sur le bouton **Enregistrer dans le modèle**.
5. Réalisez les actions suivantes dans la boîte de dialogue **Propriétés du modèle** (cf. ill. 23) :
   - Dans le champ **Nom du modèle**, saisissez le nom du modèle.
   - Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.

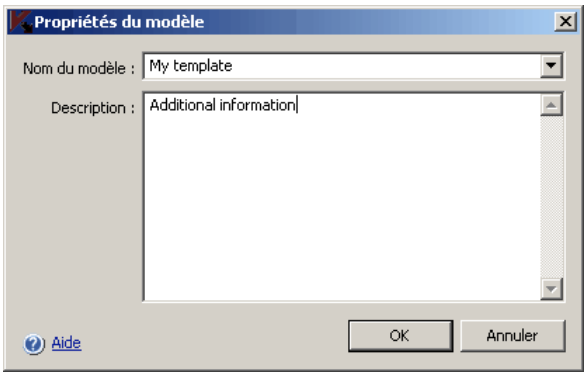

Illustration 23. Boîte de dialogue **Propriétés du modèle**

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

6.2.2.3.2. Consultation des paramètres de sécurité du modèle

Pour consulter les valeurs des paramètres de sécurité dans le modèle créé :

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez la commande **Modèles** (cf. ill. 24).

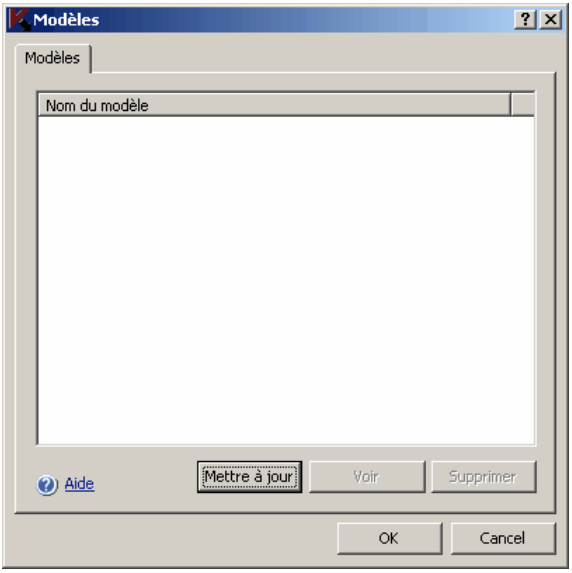

Illustration 24. Boîte de dialogue **Modèles**

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

3. Pour consulter les informations relatives au modèle et les valeurs des paramètres de sécurité, sélectionné le modèle requis dans la liste et cliquez sur le bouton **Voir** (cf. ill. 25).

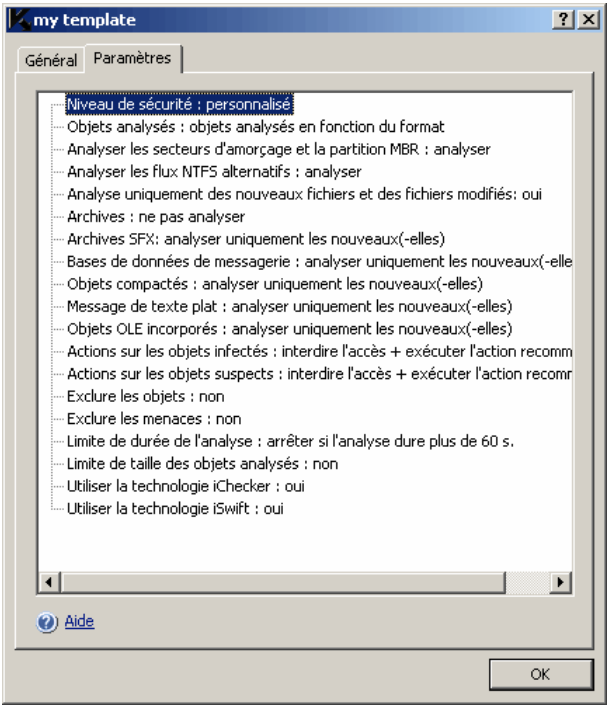

Illustration 25. Boîte de dialogue **<Nom du modèle>**, onglet **Paramètres**

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

6.2.2.3.3. Application du modèle

Pour appliquer le modèle avec la sélection de paramètre de sécurité au noeud sélectionné :

1. Enregistrez tout d'abord la sélection des valeurs des paramètres de sécurité dans le modèle (cf. instructions au point 6.2.2.3.1, p. 87).
2. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** et sélectionnez le noeud subalterne **Protection en temps réel des fichiers**.
3. Accédez au panneau des résultats, dans l'arborescence des ressources fichier du serveur, ouvrez le menu contextuel du menu du noeud auquel

vous souhaitez appliquer le modèle et sélectionnez **Appliquer un modèle**.

4. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez appliquer.
5. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

Application

Si vous appliquez le modèle au nœud parent, alors les paramètres de sécurité du modèle seront appliqués à tous les nœuds enfants, sauf ceux pour lesquels vous avez configurés les paramètres de sécurité séparément.

Pour installer les paramètres de sécurité du modèle à tous les nœuds enfants, désélectionnez la case en regard du nœud parent dans l'arborescence des ressources fichier du serveur avant d'appliquer le modèle puis cochez-la à nouveau. Appliquez le modèle au nœud parent. Tous les nœuds enfants auront les mêmes paramètres de sécurité que le nœud parent.

6.2.2.3.4. Suppression du modèle

Pour supprimer un modèle :

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez la commande **Modèles** (cf. ill. 24).
3. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez supprimer dans la liste et cliquez sur **Supprimer**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**. Le modèle sélectionné sera supprimé.

6.2.3. Sélection du mode de protection des objets

Vous pouvez sélectionner le mode de protection des objets dans la tâche **Protection en temps réel des fichiers**. Pour obtenir de plus amples informations sur les paramètres du mode de protection, lisez le point B.3.1 à la page 399.

Pour sélectionner le mode de protection des objets :

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés**, sous l'onglet **Général** (cf. ill. 26), sélectionnez le mode de protection des objets que vous souhaitez activer puis cliquez sur **OK**.

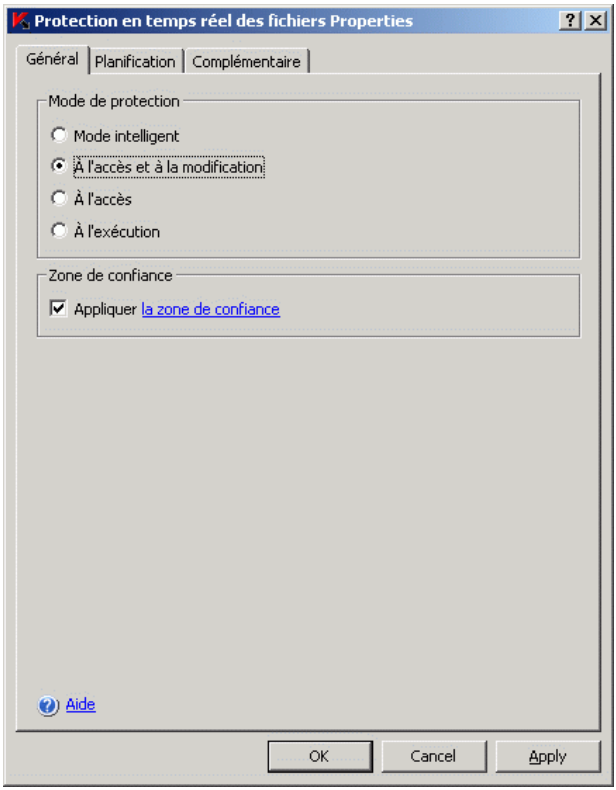

Illustration 26. Boîte de dialogue **Propriétés de la tâche**, onglet **Général**

6.3. Statistiques de la tâche *Protection en temps réel des fichiers*

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

*Pour consulter les statistiques de la tâche **Protection en temps réel des fichiers** :*

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Protection en temps réel des fichiers** et sélectionnez **Voir les statistiques**.

Dans la boîte de dialogue **État de la tâche**, vous pourrez consulter les informations suivantes sur les objets traités par Kaspersky Anti-Virus depuis son lancement jusque maintenant.

Champ	Description
Menaces détectées	Nombre de menaces détectées ; par exemple, si Kaspersky Anti-Virus a découvert un programme malveillant dans cinq objets, la valeur de ce champ augmentera d'une unité.
Objets infectés détectés	Total des objets infectés détectés.
Objets suspects détectés	Total des objets suspects détectés.
Objets non-réparés	Nombre d'objets que Kaspersky Anti-Virus n'a pas réparé parce que : a) le type de menace de l'objet ne peut être réparé b) les objets de ce type ne peuvent pas être réparés ou c) une erreur s'est produite durant la réparation.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Anti-Virus aurait du mettre en quarantaine mais sans réussir à cause d'une erreur tel que le manque d'espace sur le disque.

Champ	Description
Objets non supprimés	Nombre d'objets que Kaspersky Anti-Virus a tenté de supprimer, mais sans succès : par exemple, l'accès à l'objet est bloqué par un autre programme.
Objets non analysés	Nombre d'objets de la zone d'analyse que Kaspersky Anti-Virus n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre d'objets dont les copies auraient du être placées par Kaspersky Anti-Virus en sauvegarde mais qui n'ont pas pu l'être en raison d'une erreur.
Erreurs d'analyse	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets réparés	Nombre d'objets réparés par Kaspersky Anti-Virus.
Placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Anti-Virus.
Objets sauvegardés	Nombre d'objets dont une copie a été mise en sauvegarde par Kaspersky Anti-Virus.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Anti-Virus.
Objets protégés par mot de passe	Nombre d'objets (par exemple, archives) que Kaspersky Anti-Virus a ignoré car ils étaient protégés par un mot de passe.
Objets endommagés	Nombre d'objets ignorés par Kaspersky Anti-Virus car leur format était corrompu.
Objets analysés	Nombre total d'objets analysés par Kaspersky Anti-Virus.

6.4. Configuration de la tâche *Analyse des scripts*

La tâche prédéfinie **Analyse des scripts** possède par défaut les paramètres définis dans le tablea 4. Vous pouvez modifier les valeurs de ces paramètres et configurer la tâche.

Tableau 4. Paramètres par défaut de la tâche *Analyse des scripts*

Paramètre	Valeur par défaut	Description
Exécution des scripts infectés	Interdit	Kaspersky Anti-Virus interdit toujours l'exécution des scripts qu'il considère infectés.
Exécution des scripts suspects	Interdit	Vous pouvez définir les actions que Kaspersky Anti-Virus exécutera sur les scripts qu'il considère suspect : bloquer ou non leur exécution.
Zone de confiance	Appliquée La liste des exclusions est vide	Seule liste d'exclusions que vous pouvez appliquer dans la tâche **Analyse des scripts**. Le Chapitre 8 à la page 109 contient des informations sur la création et l'application de la zone de confiance.

*Pour configurer l'analyse de la tâche **Analyse des scripts**:*

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Analyse des scripts** et sélectionnez l'option **Propriétés**.

   La boîte de dialogue **Propriétés: Analyse des scripts** s'ouvre :
3. Dans le groupe de paramètres **Actions sur les scripts suspects**, autorisez ou interdisez l'exécution des scripts :
   - Pour autoriser l'exécution des scripts suspects, sélectionnez l'option **Autoriser l'exécution** ;

- Pour interdire l'exécution des scripts suspects, sélectionnez l'option **Interdire l'exécution**.

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

   - Pour activer l'application de la zone de confiance, cochez la case **Appliquer la zone de confiance** ;
   - Pour désactiver l'application de la zone de confiance, désélectionnez la case **Appliquer la zone de confiance**.

     Pour savoir comment ajouter des scripts à la liste des exclusions de la zone de confiance, lisez le point 8.2.3 à la page. 116.

5. Dans la boîte de dialogue **Propriétés: Analyse des scripts**, cliquez sur **OK** pour enregistrer les modifications.

6.5. Statistiques de la tâche *Analyse des scripts*

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

Pour consulter les statistiques de la tâche :

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Ouvrez le menu contextuel de la tâche **Analyse des scripts** et sélectionnez **Voir les statistiques**.

La boîte de dialogue **État de la tâche** contient les informations suivantes :

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

CHAPITRE 7. INTERDICTION DE L'ACCES DES ORDINATEURS DANS LA TACHE PROTECTION EN TEMPS REEL DES FICHIERS

Le présent chapitre aborde les sujets suivants :

- Interdiction manuelle de l'accès des ordinateurs au serveur protégé (cf. point 7.1, p. 97) ;
- Activation ou désactivation automatique de l'interdiction de l'accès des ordinateurs (cf. point 7.2, p. 98) ;
- Configuration des paramètres d'interdiction automatique de l'accès des ordinateurs (cf. point 7.3, p. 99) ;
- Exclusion des ordinateurs de la liste d'interdiction (composition de la liste des ordinateurs de confiance) (cf. point 7.4, p. 101) ;
- Prévention des épidémies virales (cf. point 7.5, p. 102) ;
- Consultation de la liste des ordinateurs dont l'accès au serveur est interdit (cf. point 7.6, p. 104) ;
- Interdiction manuelle de l'accès des ordinateurs (cf. point 7.7, p. 105) ;
- Levée de l'interdiction de l'accès des ordinateurs (cf. point 7.8, p. 107) ;
- Consultation des statistiques de l'interdiction (cf. point 7.9, p. 107).

7.1. Interdiction de l'accès des ordinateurs au serveur protégé

Pendant l'exécution de la tâche **Protection en temps réel des fichiers**, vous pouvez interdire temporairement l'accès des ordinateurs infectés au serveur protégé.

Vous pouvez interdire l'accès des ordinateurs de deux manières :

- **activer l'interdiction automatique l'accès des ordinateurs**. Dès qu'un ordinateur du réseau tente d'écrire un objet infecté ou suspect sur le serveur protégé, Kaspersky Anti-Virus attribue l'état *infecté* à l'ordinateur et exécute les actions que vous avez définies : interdiction temporaire de l'accès de l'ordinateur aux fichiers du serveur et/ou exécution du fichier exécutable indiqué. Par défaut, l'interdiction automatique de l'accès des ordinateurs est désactivée ;
- **interdire manuellement l'accès des ordinateurs infectés**. Si vous savez qu'un ordinateur de l'intranet est infecté, vous pouvez l'empêcher manuellement d'accéder au serveur protégé : ajouter l'ordinateur à la liste d'interdiction et indiquer la période pendant laquelle il ne pourra pas accéder aux objets sur le serveur protégé.

Vous pouvez lever l'interdiction d'accès de l'ordinateur au serveur à n'importe quel moment.

Toutes les opérations liées à l'interdiction ou à la levée d'interdiction de l'accès des ordinateurs sont consignées dans le journal d'audit système.

La liste des ordinateurs débloqués automatiquement est conservée entre chaque séance de fonctionnement de Kaspersky Anti-Virus.

7.2. Activation ou désactivation de l'interdiction automatique d'accès des ordinateurs

Pour activer ou désactiver la fonction d'interdiction d'accès des ordinateurs :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel**, puis le noeud **Protection en temps réel des fichiers**, afin d'afficher le noeud subalterne **Interdire l'accès des ordinateurs**.
2. Exécutez une des actions suivantes :
   - Pour activer le blocage automatique de l'accès des ordinateurs au serveur, cliquez avec le bouton droit de la souris sur l'entrée **Blocage de l'accès des ordinateurs** et sélectionnez la commande **Activer le blocage de l'accès des ordinateurs**.
   - Pour désactiver le blocage automatique de l'accès des ordinateurs au serveur, cliquez avec le bouton droit de la souris sur l'entrée **Blocage de l'accès des ordinateurs** et sélectionnez la commande **Désactiver le blocage de l'accès des ordinateurs**.
3. Cliquez sur le bouton **OK**.

Remarque

Si vous activez la fonction d'interdiction automatique de l'accès des ordinateurs, elle sera appliquée uniquement lorsque la tâche **Protection en temps réel des fichiers** est exécutée.

Dès que vous désactivez la fonction d'interdiction automatique, tous les ordinateurs pourront accéder aux fichiers sur le serveur.

7.3. Configuration des paramètres d'interdiction automatique de l'accès des ordinateurs

Cette rubrique décrit comment activer et configurer l'interdiction automatique de l'accès des ordinateurs au serveur. Une description des paramètres d'interdiction est proposée au point B.4 à la page 416.

Pour configurer les paramètres d'interdiction automatique de l'accès des ordinateurs :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel**, puis le noeud **Protection en temps réel des fichiers**, afin d'afficher le noeud subalterne **Interdire l'accès des ordinateurs**.
2. Ouvrez le menu contextuel du noeud **Interdire l'accès des ordinateurs** puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : interdire l'accès des ordinateurs**, assurez-vous que la case **Activer l'interdiction d'accès des ordinateurs au serveur** de l'onglet **Général** (cf. ill. 27).

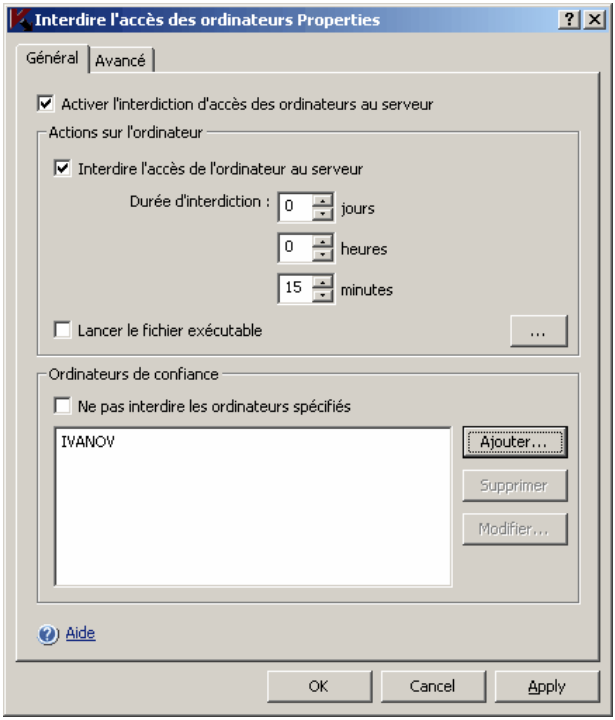

Illustration 27. Boîte de dialogue **Propriétés: Interdire l'accès des ordinateurs**, onglet **Général**

4. Dans le groupe de paramètres **Actions sur l'ordinateur**, cochez les cases en regard des actions que Kaspersky Anti-Virus exécutera lors des tentatives d'écriture d'un objet infecté ou potentiellement infecté sur le serveur depuis un ordinateur (B.4.2 à la page 417).

5. Si vous avez sélectionné **Interdire l'accès de l'ordinateur au serveur**, définissez la durée de la période (en jours, heures ou minutes) pendant laquelle vous souhaitez bloquer l'accès des ordinateurs au serveur.

6. Si vous avez sélectionné l'option **Lancer le fichier exécutable**, cliquez sur le bouton de la liste  et dans la boîte de dialogue **Fichier exécutable** (cf. ill. 28), indiquez le fichier exécutable (son nom ou le chemin d'accès complet) ainsi que le compte utilisateur sous les privilèges duquel le fichier exécutable sera lancé.

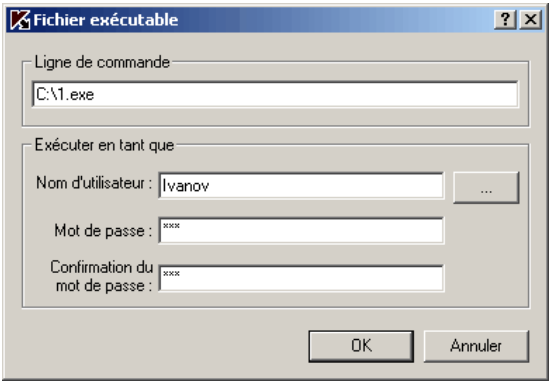

Illustration 28. Boîte de dialogue **Fichier exécutable**

7. Cliquez sur **OK**.

7.4. Exclusion d'ordinateurs de l'interdiction automatique (ordinateurs de confiance)

Vous pouvez composer une liste d'ordinateurs de confiance (pour de plus amples informations sur le paramètre, lisez le point B.4.3 à la page 419).

Pour ajouter un ordinateur à la liste des ordinateurs de confiance :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel**, puis le noeud **Protection en temps réel des fichiers**, afin d'afficher le noeud subalterne **Interdire l'accès des ordinateurs**.
2. Ouvrez le menu contextuel du noeud **Interdire l'accès des ordinateurs** puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés: Interdire l'accès des ordinateurs**, assurez-vous que la case **Activer l'interdiction d'accès des ordinateurs au serveur** de l'onglet **Général** (cf. ill. 27) est cochée (cf. point B.4.1, p. 417).
4. Dans le groupe de paramètres **Ordinateurs de confiance**, cochez la case **Ne pas interdire les ordinateurs spécifiés** et exécutez les actions suivantes :

a) Cliquez sur **Ajouter**. La boîte de dialogue Ajouter un ordinateur s'ouvre (cf. ill. 29).

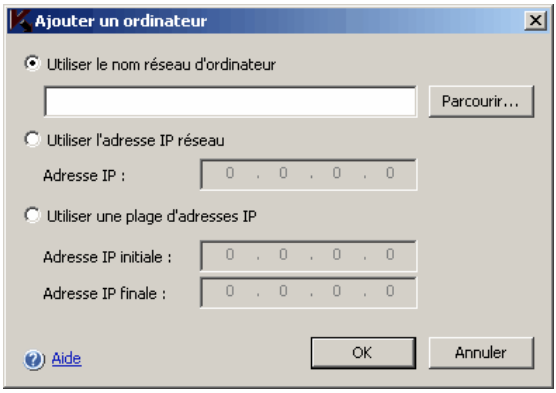

Illustration 29. Boîte de dialogue **Ajouter un ordinateur**

b) Indiquez le nom de réseau ou l'adresse IP de l'ordinateur :

- Sélectionnez **Utiliser le nom réseau d'ordinateur** et indiquez le nom NetBIOS de l'ordinateur ;
- Indiquez l'adresse IP statique : Sélectionnez **Utiliser l'adresse IP réseau** et saisissez l'adresse IP de l'ordinateur ;
- Saisissez la plage d'adresses IP : Sélectionnez **Utiliser une plage d'adresses IP**, saisissez la première adresse IP de la plage dans le champ **Adresse IP initiale** et la dernière adresse IP dans le champ **Adresse IP finale**. Tous les ordinateurs dont l'adresse IP appartient à la plage indiquée seront considérés comme des ordinateurs de confiance.

c) Cliquez sur **OK**.

5. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés**.

7.5. Prévention des épidémies virales

Cette section décrit comment activer ou désactiver la prévention des épidémies virales. La fonction *Prévention des épidémies virales* est décrite au point B.4.4 à la page 419.

Pour activer/désactiver la prévention des épidémies virales :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel**, puis le noeud **Protection en temps réel des fichiers**, afin d'afficher le noeud subalterne **Interdire l'accès des ordinateurs**.
2. Ouvrez le menu contextuel du noeud **Interdire l'accès des ordinateurs** puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : interdire l'accès des ordinateurs** , ouvrez l'onglet **Avancé** (cf. ill. 30).

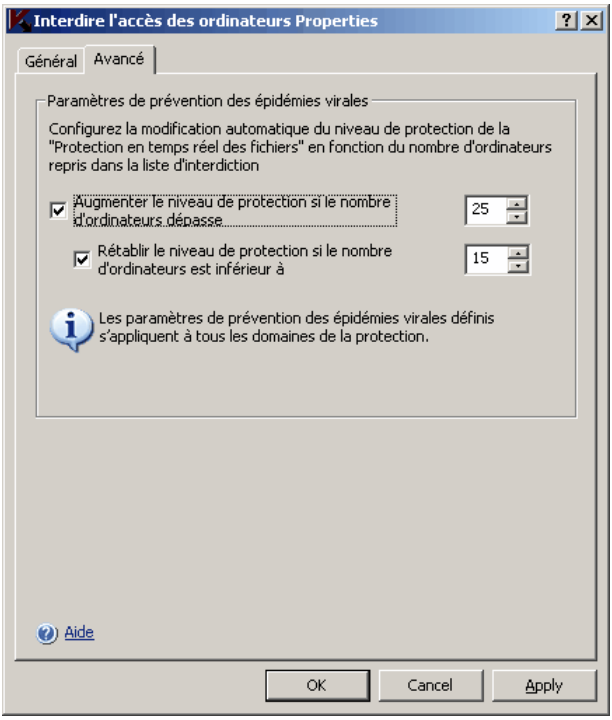

Illustration 30. Boîte de dialogue **Interdire l'accès des ordinateurs**, onglet **Avancé**

4. Sur l'onglet **Avancé** , exécutez une des actions suivantes.
   - Pour activer la prévention des épidémies virales :
     a) Cochez la case **Augmenter le niveau de protection si le nombre d'ordinateurs dépasse**.

b) Définissez le nombre d'ordinateurs repris dans la liste d'interdiction qui, une fois atteint, entraînera le renforcement de la protection offerte par Kaspersky Anti-Virus.

c) Le cas échéant, activez la restauration du niveau de protection lorsque le niveau d'ordinateurs interdits d'accès est à nouveau égal au nombre du champ **Rétablir le niveau de protection si le nombre d'ordinateurs est inférieur à**.

- Pour désactiver la prévention des épidémies de virus, désélectionnez **Augmenter le niveau de protection si le nombre d'ordinateurs dépasse**.

5. Cliquez sur **OK**.

7.6. Consultation de la liste des ordinateurs dont l'accès au serveur est interdit

Attention !

Les ordinateurs repris dans la liste d'interdiction d'accès au serveur ne peuvent accéder au serveur protégé uniquement lorsque la tâche **Protection en temps réel des fichiers** est exécutée et que la fonction d'interdiction automatique de l'accès des ordinateurs est activée.

Pour consulter la liste des ordinateurs qui ne peuvent accéder pour l'instant au serveur protégé :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** puis, le noeud **Protection en temps réel des fichiers**.
2. Ouvrez le noeud subalterne **Interdire l'accès des ordinateurs** (cf. ill. 31).

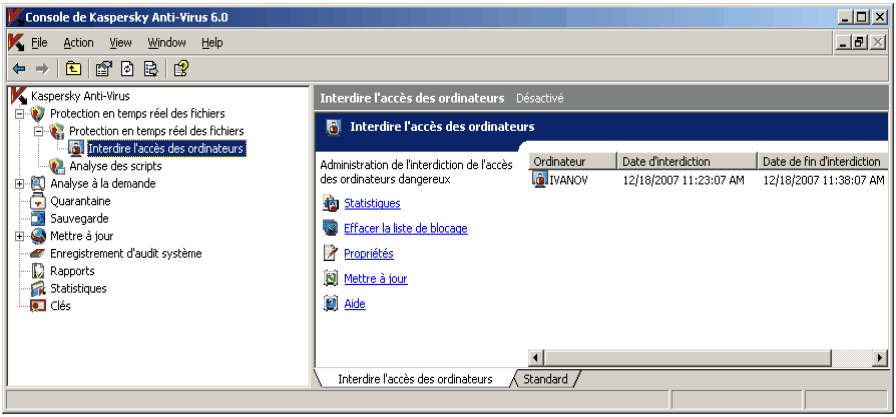

Illustration 31. Fenêtre **Interdire l'accès des ordinateurs**

Le panneau des résultats affiche les informations suivantes relatives aux ordinateurs dont l'accès au serveur reste interdit :

Champ	Description
Nom de l'ordinateur	Informations relatives à l'ordinateur dans la liste de blocage, obtenues par Kaspersky Anti-Virus (nom de réseau, adresse IP de l'ordinateur).
Date d'interdiction	Date et heure où l'ordinateur a été interdit ; ces données sont affichées selon les paramètres de la configuration régionale de Microsoft Windows de l'ordinateur où est installée la console de Kaspersky Anti-Virus.
Date de fin d'interdiction	Date et heure où l'accès de l'ordinateur a été autorisé ; ces données sont affichées selon les paramètres de la configuration régionale de Microsoft Windows de l'ordinateur où est installée la console de Kaspersky Anti-Virus.

7.7. Interdiction manuelle de l'accès des ordinateurs

Si vous savez qu'un ordinateur de l'intranet est infecté, vous pouvez l'empêcher manuellement d'accéder au serveur protégé.

Attention !

Les ordinateurs repris dans la liste d'interdiction d'accès ne peuvent accéder au serveur protégé uniquement lorsque la tâche **Protection en temps réel des fichiers** est exécutée et que l'interdiction automatique de l'accès des ordinateurs est activée.

Pour interdire manuellement l'accès de l'ordinateur au serveur :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** puis, le noeud **Protection en temps réel des fichiers**.
2. Assurez-vous que l'interdiction automatique de l'accès depuis les ordinateurs est activée (cf. point 7.2, p. 98).
3. Ouvrez le menu contextuel du noeud subalterne **Interdire l'accès des ordinateurs** et sélectionnez **Ajouter à la liste d'interdiction**.
4. Dans la boîte de dialogue **Ajout de l'ordinateur à la liste d'interdiction** (cf. ill. 32), indiquez le nom de réseau de l'ordinateur que vous souhaitez empêcher d'accéder au serveur.

Remarque

Dans le champ **Nom de l'ordinateur**, indiquez uniquement les noms de réseau NetBIOS des ordinateurs et n'indiquez pas les adresses DNS.

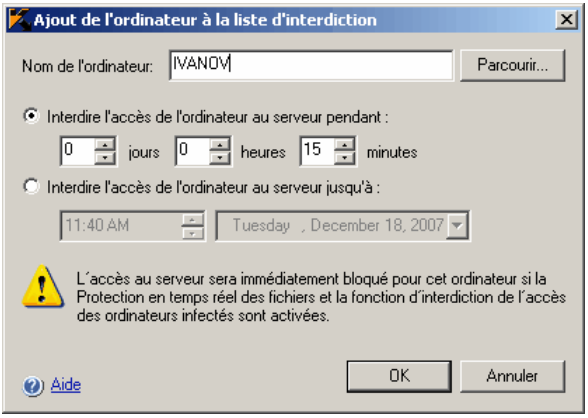

Illustration 32. Boîte de dialogue **Ajout de l'ordinateur à la liste d'interdiction**

5. Exécutez une des actions suivantes :

- Sélectionnez **Interdire l'accès de l'ordinateur au serveur pendant** et définissez l'intervalle de temps pendant lequel l'ordinateur ne pourra pas accéder au serveur ;
- Sélectionnez **Interdire l'accès de l'ordinateur au serveur jusqu'à** pour définir la date et l'heure de la fin de l'interdiction de l'accès de l'ordinateur.

6. Cliquez sur **OK**.

7.8. Levée de l'interdiction de l'accès des ordinateurs

Vous pouvez lever l'interdiction d'accès de l'ordinateur au serveur protégé à n'importe quel moment.

Pour autoriser l'accès d'un ordinateur :

1. Dans l'arborescence de la console, déployez le noeud **Protection en temps réel** puis, le noeud **Protection en temps réel des fichiers**.
2. Sélectionnez le noeud subalterne **Interdire l'accès des ordinateurs**.
3. Dans la fenêtre **Interdire l'accès des ordinateurs**, dans la liste des ordinateurs interdits, ouvrez le menu contextuel de la ligne contenant les informations relatives à l'ordinateur pour lequel vous souhaitez lever l'interdiction et sélectionnez **Autoriser l'accès de l'ordinateur**.

7.9. Consultation des statistiques de l'interdiction

Vous pouvez consulter les informations relatives au nombre d'ordinateurs dont l'accès au serveur protégé a été interdit depuis la dernière exécution de Kaspersky Anti-Virus . Il s'agit des *statistiques d'interdiction*.

Pour consulter les statistiques d'interdiction :

1. Dans l'arborescence de la console, développez le noeud **Protection en temps réel**.
2. Déployez le noeud **Protection en temps réel des fichiers**.
3. Ouvrez le menu contextuel du noeud **Interdire l'accès des ordinateurs** puis, sélectionnez **Voir les statistiques** (cf. ill. 33).

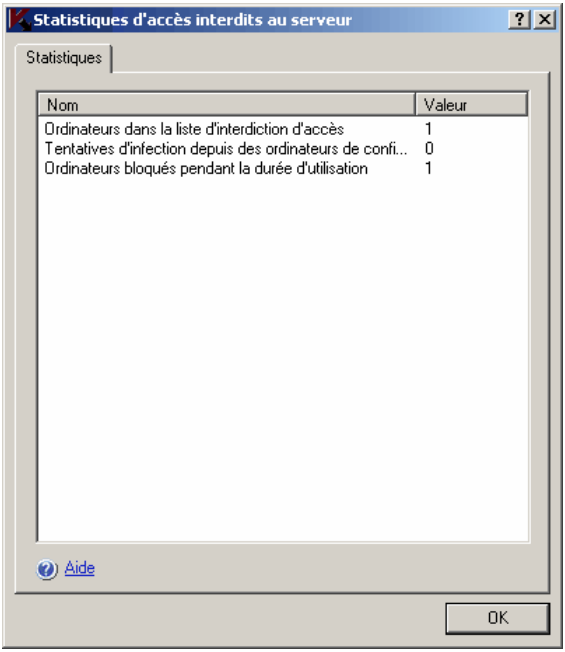

Illustration 33. Boîte de dialogue **Statistiques d'accès interdits au serveur**

La boîte de dialogue **Statistiques d'accès interdits au serveur** contient les informations suivantes :

Champ	Description
Ordinateurs dans la liste d'interdiction d'accès	Nombre d'ordinateurs dans la liste d'interdiction d'accès à ce moment
Tentatives d'infection depuis des ordinateurs de confiance	Nombre de tentatives d'écriture d'objets infectés ou suspects des ordinateurs de confiance sur le serveur depuis l'activation de la fonction d'interdiction automatique
Nombre total d'ordinateurs dans la liste d'interdiction d'accès	Nombre total d'ordinateurs ajouté à la liste d'interdiction automatique d'accès lors d'une tentative d'écriture d'objets infectés ou suspects sur le serveur depuis l'activation de la fonction d'interdiction automatique

CHAPITRE 8. ZONE DE CONFIANCE

Le présent chapitre aborde les sujets suivants :

- Présentation de la zone de confiance de Kaspersky Anti-Virus (cf. point 8.1, p. 109) ;
- Ajout d'exclusions à la zone de confiance (cf. 8.2 à la page 111) ;
- Application de la zone de confiance (cf. point 8.3, p. 120).

8.1. Présentation de la zone de confiance de Kaspersky Anti-Virus

Vous pouvez composer une liste unique d'exclusion de la zone de protection (analyse) et, quand les conditions l'imposent, appliquer ces exclusions aux tâches d'analyse à la demande sélectionnées et à la tâche **Protection en temps réel des fichiers**. Cette liste d'exclusion s'appelle la *zone de confiance*.

La zone de confiance de Kaspersky Anti-Virus peut reprendre les objets suivants :

- les fichiers sollicités par les processus des applications et sensibles aux interceptions de fichiers (*processus de confiance*),
- les fichiers auxquels on accède durant les opérations de copie de sauvegarde (*opérations de copie de sauvegarde*) et
- les objets indiqués par l'utilisateur en fonction de leur emplacement et/ou de la menace (*règles d'exclusion*).

Par défaut, la zone de confiance est appliquée dans les tâches **Protection en temps réel des fichiers** et **Analyse des scripts** ; dans les tâches prédéfinies ou définies par l'utilisateur d'analyse à la demande.

Processus de confiance (appliqués uniquement dans la tâche **Protection en temps réel des fichiers**)

Certaines applications du serveur peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par un logiciel antivirus. Les

contrôleurs de domaine sont un exemple d'applications appartenant à cette catégorie.

Afin de ne pas perturber la stabilité de telles applications, vous pouvez désactiver la protection en temps réel des fichiers sollicités par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Microsoft Corporation recommande d'exclure ces applications de la protection en temps réel des fichiers sous prétexte que certaines de celles-ci ne sont pas exposées à l'infection. Vous pouvez consulter la liste des fichiers dont l'exclusion est recommandée sur le site de Microsoft Corporation http://www.microsoft.com/fr/fr/, code l'article : KB822158.

Vous pouvez appliquer une zone de confiance avec la fonction *Processus de confiance* ou sans celle-ci.

N'oubliez pas que si le fichier exécutable du processus change, par exemple s'il est actualisé, alors Kaspersky Anti-Virus l'excluera de la liste des applications de confiance.

Opérations de copie de sauvegarde (application uniquement dans la tâche **Protection en temps réel des fichiers**)

Pendant la création d'une copie de sauvegarde des fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités durant les opérations de copie de sauvegarde. Kaspersky Anti-Virus n'analyse pas les fichiers que l'application de sauvegarde ouvre en lecteur avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Vous pouvez appliquer une zone de confiance en désactivant la protection en temps réel des fichiers durant la sauvegarde ou sans celle-ci.

Règles d'exclusions (appliquée dans les tâches **Protection en temps réel des fichiers** et **Analye des scripts** et dans les tâches d'analyse à la demande)

Vous pouvez exclure des objets de l'analyse dans des tâches particulières sans utiliser une zone de confiance ou vous pouvez conserver une liste unique d'exclusions dans la zone de confiance et, quand la situation l'impose, appliquer ces exclusions dans les tâches sélectionnées : **Protection en temps réel des fichiers** et **Analye des scripts** et dans les tâches d'analyse à la demande.

Vous pouvez ajouter à la zone de confiance des objets en fonction de leur emplacement sur le serveur, en fonction du nom de la menace identifée dans ceux-ci ou selon une combinaison de ces deux éléments.

Lorsque vous ajoutez une nouvelle exclusion à la zone de confiance, vous définissez une règle (les indices selon lesquels Kaspersky Anti-Virus ignorera les objets) et indiquez à quelles tâches (**Protection en temps réel des**

fichiers, Analyse des scripts et/ou **Analyse à la demande**) cette règle s'appliquera.

En fonction de la règle que vous avez définie, Kaspersky Anti-Virus peut ignorer dans les composants indiqués :

- Les menaces définies dans les secteurs indiqués du serveur ;
- Toutes les menaces dans les secteurs indiqués du serveur ;
- Les menaces définies dans toute la couverture d'analyse.

Si vous avez choisi lors de l'installation de Kaspersky Anti-Virus l'option **Ajouter les programmes d'administration à distance aux exclusions** et **Ajouter les fichiers recommandés par Microsoft aux exclusions**, alors ces règles d'exclusion seront appliquées dans la tâche **Protection en temps réel des fichiers** ainsi que dans les tâches prédéfinies d'analyse à la demande à l'exception des tâches **Analyse des objets en quarantaine** et **Vérification de l'intégrité de l'application**.

8.2. Ajout d'exclusions à la zone de confiance

Cette section aborde les sujets suivants :

- Ajout de processus à la liste des processus de confiance (cf. point 8.2.1, p. 111) ;
- Désactivaton de la protection en temps réel des fichiers pendant la création de la sauvegarde (cf. point 8.2.2, p. 115) ;
- Ajout de règles d'exclusion (cf. point 8.2.3, p 116).

8.2.1. Ajout de processus à la liste des processus de confiance

Afin de ne pas perturber la stabilité des applications sensibles aux interceptions de fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Vous pouvez ajouter un processus à la liste des processus de confiance d'une des manières suivantes :

- Sélectionner ce processus dans la liste des processus exécutés actuellement sur le serveur protégé ;
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

Remarque

Si le fichier exécutable du processus change, Kaspersky Anti-Virus l'exclut de la liste des processus de confiance.

Pour ajouter un processus à la liste des processus de confiance :

1. Dans la console de Kaspersky Anti-Virus dans MMC, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.
2. Dans la boîte de dialogue **Zone de confiance**, sur l'onglet **Processus de confiance** (cf. Illustration 34), activez la fonction *Processus de confiance* : cochez la case **Ne pas surveiller l'activité sur fichiers des processus spécifiés**.

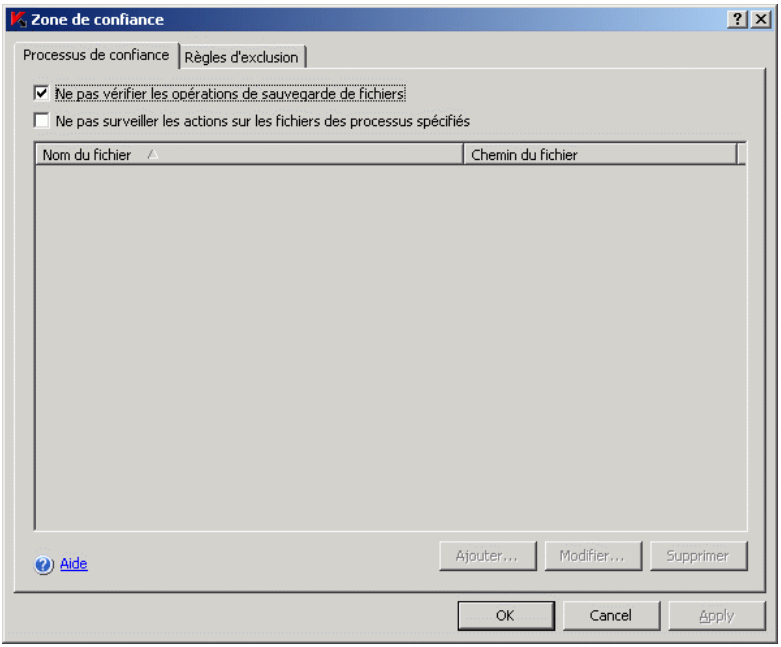

Illustration 34. Boîte de dialogue **Zone de confiance**, onglet **Processus de confiance**

3. Ajoutez le processus de confiance de la liste des processus exécutés ou indiquez le fichier exécutable du processus.

   - Pour ajouter un processus au départ de la liste des processus exécutés :

     a) Cliquez sur **Ajouter**.

     b) Dans la boîte de dialogue **Ajout d'un processus de confiance** (cf. Illustration 35), cliquez sur le bouton **Processus**.

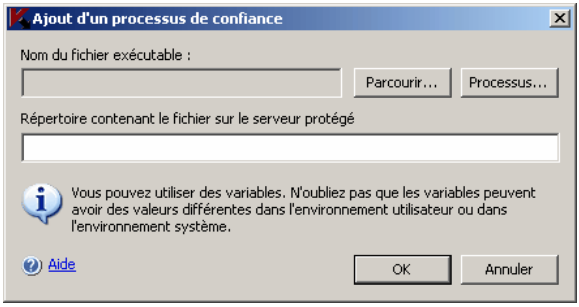

Illustration 35. Boîte de dialogue **Ajout d'un processus de confiance**

     c) Dans la boîte de dialogue **Processus actifs** (cf. Illustration 36) sélectionnez le processus souhaité et cliquez sur **OK**.

        Pour trouver le processus souhaité dans la liste, vous pouvez trier les processus par nom, par PID ou par chemin au fichier exécutable du processus.

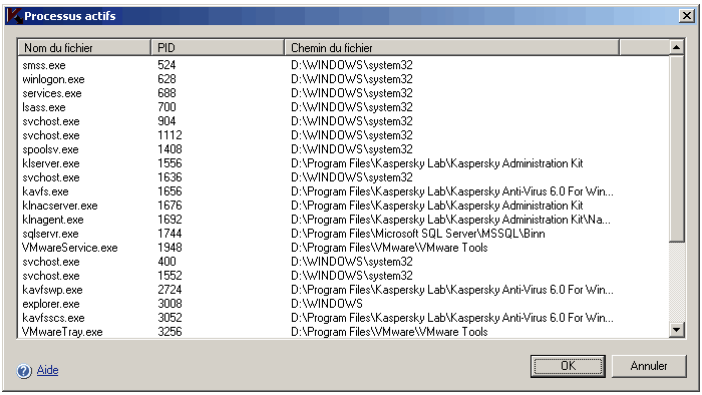

Illustration 36. Boîte de dialogue **Processus actifs**

Remarque

Vous devez faire partie du groupe des administrateurs locaux sur le serveur protégé afin de consulter les processus actifs sur celui-ci.

Le processus sélectionné sera ajouté à la liste des processus de confiance dans la boîte de dialogue **Processus de confiance**.

- Pour sélectionner le fichier exécutable du processus sur le disque du serveur protégé, procédez de la manière suivante :

  a) Sur l'onglet **Processus de confiance**, cliquez sur le bouton **Ajouter**.

  b) Dans la boîte de dialogue **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du processus sur le disque local du serveur protégé. Cliquez sur **OK**.

  Le nom du fichier et le chemin d'accès à celui-ci apparaît dans la boîte de dialogue **Ajout d'un processus de confiance**.

  Remarque

  Kaspersky Anti-Virus ne considèrera pas un processus comme un processus de confiance si le chemin d'accès au fichier exécutable du processus est différent du chemin d'accès que vous avez saisi dans le champ **Chemin du fichier**. Si vous souhaitez que le processus exécuté depuis un fichier situé dans n'importe quel dossier soit considéré comme un processus de confiance, saisissez le caractère * dans le champ **Chemin du fichier**. Vous pouvez utiliser des variables dans le chemin.

  c) Cliquez sur **OK**.

  Le nom du fichier exécutable du processus sélectionné apparaît dans la liste des processus de confiance de l'onglet **Processus de confiance**.

4. Cliquez sur **OK** pour enregistrer les modifications.
5. Vérifiez que la zone de confiance est bien appliquée dans la tâche **Protection en temps réel des fichiers** (cf. point 8.3, p. 120).

8.2.2. Désactivation de la protection en temps réel des fichiers durant la copie de sauvegarde

Pendant la création d'une copie de sauvegarde des fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités durant les opérations de copie de sauvegarde. Kaspersky Anti-Virus n'analyse pas les fichiers que l'application de sauvegarde ouvre en lecteur avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Remarque

Les informations relatives aux nombres de fichiers que Kaspersky Anti-Virus ignore dans les opérations de sauvegarde n'apparaît pas dans la boîte de dialogue **Statistiques** de la tâche **Protection en temps réel des fichiers**.

Pour désactiver la protection en temps réel des fichiers durant la copie de sauvegarde :

1. Dans la console de Kaspersky Anti-Virus dans MMC, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.
2. Dans la boîte de dialogue **Zone de confiance**, onglet **Processus de confiance**, exécutez une des actions suivantes :
   - Pour désactiver la protection en temps réel des fichiers sollicités pendant la copie de sauvegarde, cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.
   - Pour activer la protection en temps réel des fichiers sollicités pendant la copie de sauvegarde, désélectionnez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.
3. Cliquez sur **OK** pour enregistrer les modifications.
4. Vérifiez que la zone de confiance est bien appliquée dans la tâche **Protection en temps réel des fichiers** (cf. point 8.3, p. 120).

8.2.3. Ajout de règles d'exclusion

Pour ajouter une règle d'exclusion :

1. Dans la console de Kaspersky Anti-Virus dans MMC, ouvrez le menu contextuel du composant enfichable de Kaspersky Anti-Virus et sélectionnez la commande **Configurer la zone de confiance**.
2. Sur l'onglet **Règles d'exclusion** de la fenêtre **Zone de confiance**, cliquez sur le bouton **Ajouter**.

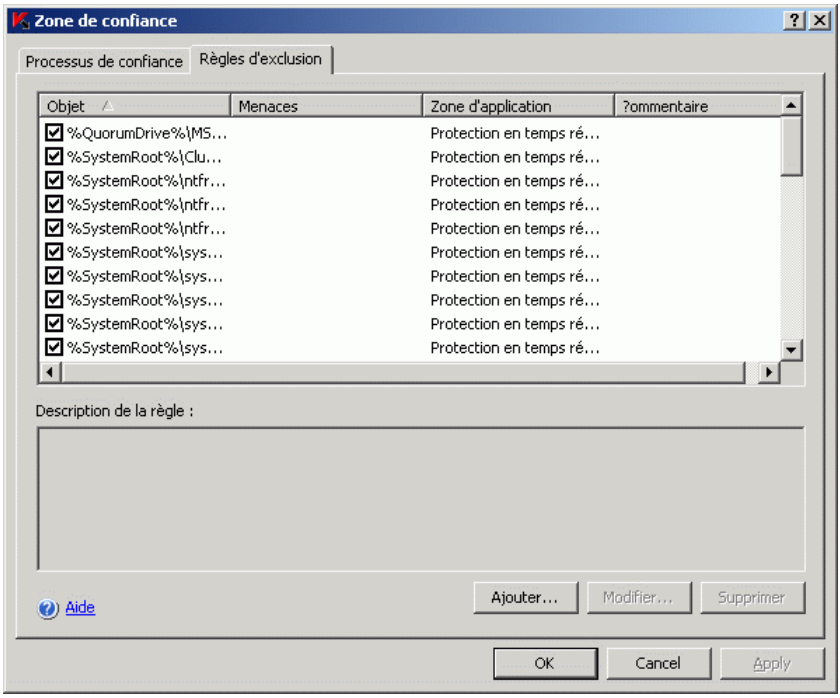

Illustration 37. Boîte de dialogue **Zone de confiance**, onglet **Règles d'exclusions**

La boîte de dialogue **Règle d'exclusion** s'ouvre.

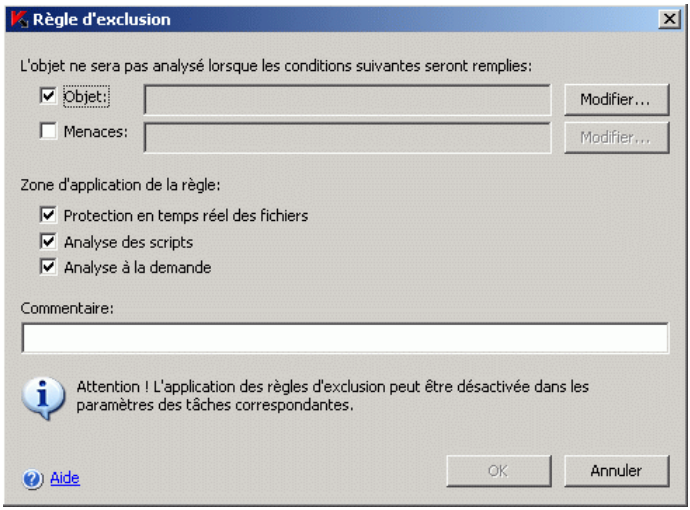

Illustration 38. Boîte de dialogue **Règle d'exclusion**

3. Indiquez la règle selon laquel Kaspersky Anti-Virus va exclure les objets.

Remarque

Pour exclure *les menaces définies dans les secteurs indiqués*, cochez les cases **Objet** et **Menaces**.

Pour exclure *toutes les menaces dans les secteurs indiqués*, cochez la case **Objet** et désélectionnez la case **Menaces**.

Pour exclure *les menaces définies dans toute la couverture d'analyse*, désélectionnez la case **Objet** et cochez la case **Menaces**.

- *Si vous souhaitez indiquer l'emplacement de l'objet*, cochez la case **Objet**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Sélection de l'objet** (cf. ill 39), sélectionnez l'objet qui sera exclu de l'analyse puis cliquez sur **OK** :
  - **Zone d'analyse prédéfinie**. Sélectionnez une des zones d'analyse prédéfinie dans la liste.
  - **Disque ou répertoire**. Indiquez le disque du serveur ou le répertoire sur le serveur ou dans le réseau local.
  - **Fichier**. Indiquez le fichier sur le serveur ou dans le réseau local.

- **Fichier ou URL du script**. Désignez le script sur le serveur protégé, dans le réseau local ou sur Internet.

> **Remarque**
>
> Vous pouvez définir des masques de nom d'objets à l'aide des caractères ? et *.

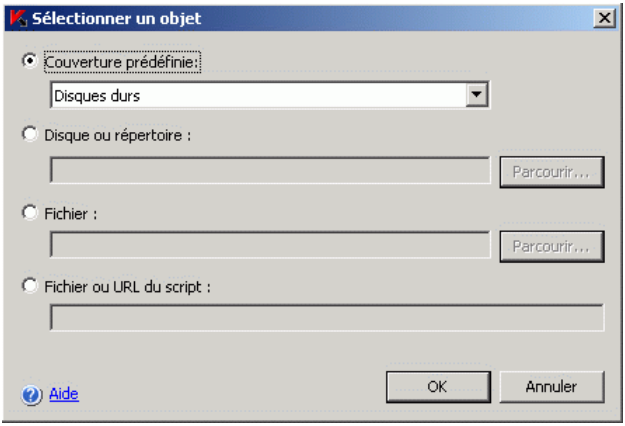

Illustration 39. Boîte de dialogue **Sélection de l'objet**

- *Si vous souhaitez définir le nom de la menace*, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Liste des exclusions** (cf. ill. 40), ajoutez les noms des menaces (pour de plus amples informations sur le paramètre, lisez le point B.3.9 à la page 411).

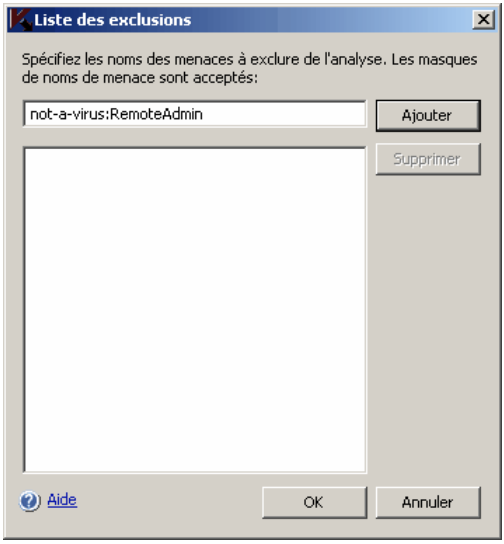

Illustration 40. Boîte de dialogue **Liste des exclusions**

4. Dans la boîte de dialogue **Règle d'exclusion**, sous l'onglet **Zone d'application de la règle**, cochez la case en regard des composants fonctionnels dans les tâches desquels la règle d'exclusion sera appliquée.
5. Cliquez sur **OK**.
   - Pour modifiez une règle, ouvrez la boîte de dialogue **Zone de confiance** et sur l'onglet **Règles d'exclusion**, sélectionnez la règle que vous souhaitez modifier, cliquez sur le bouton **Modifier** et introduisez les modifications dans la boîte de dialogue **Règle d'exclusion**.
   - Pour supprimer une règle, ouvrez la boîte de dialogue **Zone de confiance** et sur l'onglet **Règles d'exclusion**, sélectionnez la règle que vous souhaitez supprimer, cliquez sur le bouton **Supprimer** et confirmer l'opération.
6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Zone de confiance**.

8.3. Application de la zone de confiance

Par défaut, la zone de confiance est appliquée dans les tâches du composant **Protection en temps réel**, dans les tâches d'analyse à la demande prédéfinies ou recréées.

Vous pouvez activer ou désactiver l'application de la zone de confiance dans des tâches distinctes dans la boîte de dialogue **Propriétés de la tâche**.

Après que vous avez activé ou désactivé la zone de confiance, ses exclusions seront appliquées ou non immédiatement dans les tâches **Protection en temps réel des fichiers** et **Analyse des scripts**, et dans les tâches d'analyse à la demande, au prochain lancement de la tâche.

Pour appliquer les exclusions de la zone de confiance dans une tâche :

1. Dans la console MMC, ouvrez le menu contextuel sur le nom de la tâche et dans la boîte de dialogue **Propriétés de la tâche**, onglet **Général**, cochez la case **Appliquer la zone de confiance**.
2. Cliquez sur **OK**.

CHAPITRE 9. ANALYSE A LA DEMANDE

Le présent chapitre aborde les sujets suivants :

- Tâches d'analyse à la demande (cf. point 9.1, p. 121) ;
- Configuration de la tâche d'analyse à la demande (cf. 9.2, p. 122) ;
- Exécution en arrière-plan de la tâche d'analyse à la demande (cf. point 9.3, p. 145) ;
- Statistiques de la tâche d'analyse à la demande (cf. point 9.4, p. 147).

9.1. Présentation des tâches d'analyse à la demande

Kaspersky Anti-Virus prévoit quatre tâches prédéfinies d'analyse à la demande :

- La tâche **Analyse complète de l'ordinateur** est exécutée par défaut chaque semaine selon le programme défini. Kaspersky Anti-Virus analyse tous les objets du serveur protégé selon les paramètres de sécurité dont les valeurs correspondent à celles du niveau **Recommandé** (cf. point 9.2.2.1, p. 132). Vous pouvez modifier les paramètres la tâche **Analyse complète de l'ordinateur**.
- La tâche **Analyse des objets en quarantaine** est exécutée par défaut selon la programmation après chaque mise à jour des bases. Kaspersky Anti-Virus analyse le répertoire de quarantaine selon les paramètres repris au point 11.3 à la page 177. Vous ne pouvez pas modifier les paramètres de la tâche **Analyse des objets en quarantaine**.
- La tâche **Analyse au démarrage du système** est exécutée de manière programmée au démarrage du serveur. Kaspersky analyse les objets de démarrage, les modules du logiciel, les secteurs d'amorçage et les principaux enregistrements d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. Kaspersky Anti-Virus applique le niveau de protection prédéfini **Recommandé** (cf. point 9.2.2.1, p. 132). Il est possible de modifier les paramètres de la programmation ou de désactiver le lancement de cette tâche.

- La tâche **Analyse de l'intégrité de l'application** est exécutée de manière programmée au démarrage de Kaspersky Anti-Virus. Kaspersky Anti-Virus vérifie l'authenticité de ses modules exécutables. Vous ne pouvez pas modifier les paramètres la tâche **Analyse de l'intégrité de l'application**. Il est possible de modifier les paramètres de la programmation ou de désactiver le lancement de cette tâche programmée.

Vous pouvez créer des *tâches définies par l'utilisateur* dans le noeud *Analyse à la demande*. Par exemple, vous pouvez créer une tâche d'analyse du répertoire partagé sur le serveur.

Kaspersky Anti-Virus peut exécuter simultanément plusieurs tâches d'analyse à la demande.

Pour en savoir plus sur les catégories de tâches prévues dans Kaspersky Anti-Virus, en fonction de l'emplacement de la création et de l'exécution, lisez le point 5.1 à la page 54.

Pour en savoir plus sur les fonctions *Protection en temps réel* et *Analyse à la demande*, lisez le point 1.1.1 à la page 15.

Pour savoir comment administrer les tâches dans la console de Kaspersky Anti-Virus dans MMC, consulter le point Chapitre 5, page 54.

9.2. Configuration des tâches d'analyse à la demande

Vous pouvez configurer la tâche système **Analyse complète de l'ordinateur** ainsi que les tâches d'analyse à la demande définies par l'utilisateur.

Pour savoir comment créer un tâche d'analyse à la demande définie par l'utilisateur, lisez le point 5.2 à la page 56.

Pour configurer la tâche d'analyse à la demande :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche que vous souhaitez configurer afin de l'ouvrir.
3. Configurez les paramètres de la tâche : composez la couverture d'analyse ; le cas échéant, modifiez les paramètres de sécurité de toute la couverture d'analyse ou de certains de ces nœuds Par défaut, la tâche prédéfinie **Analyse complète de l'ordinateur** ainsi que les nouvelles tâches prédéfinies par l'utilisateur possèdent les paramètres décrits au tableau 5.

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

Tableau 5. Paramètres par défaut de la tâche **Analyse complète de l'ordinateur**

Paramètre	Valeur	Configuration
Couverture de l'analyse	Tout le serveur	Vous pouvez limiter la couverture de l'analyse (cf. point 9.2.1, p. 124).
Paramètres de sécurité	Identiques pour toutes les couvertures d'analyse; correspondent au niveau de protection **Recommandé**	Pour les nœuds sélectionnés dans l'arborescence des ressources fichier du serveur, vous pouvez : • Sélectionner un autre niveau de protection prédéfini (cf. point 9.2.2.1, p. 132) ; • Modifier les paramètres de protection (cf. point 9.2.2, p. 132). Vous pouvez enregistrer les paramètres de protection du noeud sélectionné dans un modèle afin de pouvoir l'appliquer par la suite à n'importe quel autre noeud (cf. point 9.2.2.3, p. 140).

Paramètre	Valeur	Configuration
Zone de confiance	Appliquée Les programmes d'administration à distance **RemoteAdmin** sont exclus ainsi que les fichiers recommandés par Microsoft Corporation si, au moment de l'installation de Kaspersky Anti-Virus, vous avez sélectionné **Ajouter les menaces selon le masque not-a-virus:RemoteAdmin* aux exclusions** et **Ajouter les fichiers recommandés par Microsoft aux exclusions**.	Une liste unique d'exclusions que vous pouvez appliquer dans des tâches d'analyse à la demande sélectionnée et dans la tâche de **Protection en temps réel des fichiers**. Chapitre 8 à la page 109 contient des informations sur la création et l'application de la zone de confiance.

9.2.1. Couverture de l'analyse dans les tâches d'analyse à la demande

Cette section aborde les sujets suivants :

- Présentation de la constitution d'une couverture d'analyse (cf. point 9.2.1.1, p. 125) ;
- Présentation des couvertures prédéfinies (cf. point 9.2.1.2, p. 125) ;
- Constitution d'une couverture d'analyse (cf. point 9.2.1.3, p. 127) ;
- Intégration du chemin de réseau dans la couverture d'analyse (cf. point 9.2.1.4, p. 129) ;
- Création d'une couverture d'analyse virtuelle ; intégration à la couverture d'analyse des disques, des répertoires et des fichiers dynamiques (cf. point 9.2.1.5, p. 129).

9.2.1.1. Présentation de la constitution d'une couverture d'analyse dans les tâches d'analyse à la demande

Par défaut, la couverture d'analyse de la tâche prédéfinie **Analyse complète de l'ordinateur** et des nouvelles tâches d'analyse à la demande créées par l'utilisateur porte sur tout le serveur. Vous pouvez restreindre la couverture de l'analyse à certains secteurs du serveur uniquement si la politique de sécurité n'impose pas la nécessité de les analyser tous.

Dans la console de Kaspersky Anti-Virus, la couverture de l'analyse se présente sur la forme d'une arborescence des ressources fichiers du serveur que Kaspersky Anti-Virus peut analyser.

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

- ☑ Noeud repris dans la couverture d'analyse.
- ☐ Noeud exclu de la couverture d'analyse.
- ☑ Au moins un des nœuds intégrés à ce noeud est exclu de la couverture d'analyse ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du noeud de niveau supérieur.

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

9.2.1.2. Couvertures d'analyse prédéfinies

Pour consulter l'arborescence des ressources fichiers du serveur :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter la couverture d'analyse afin d'ouvrir la tâche (cf. ill. 41).

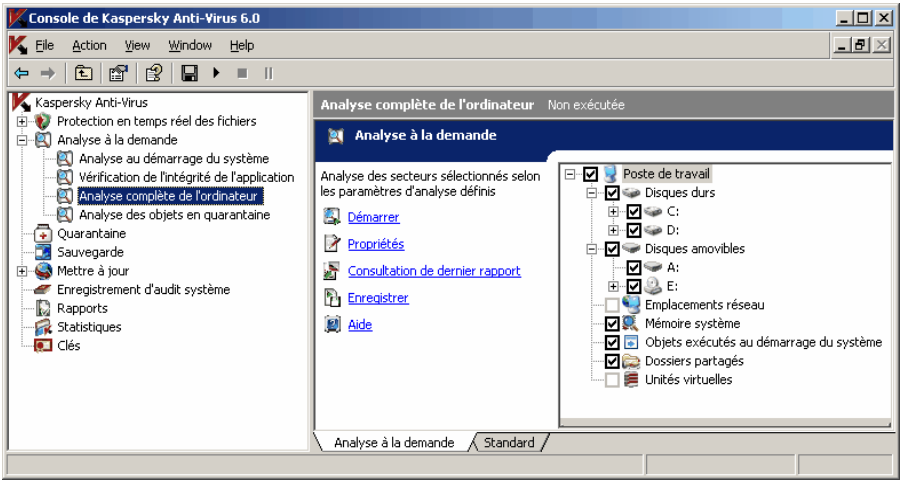

Illustration 41. Exemple d'arborescence des ressources fichier du serveur dans la console de Kaspersky Anti-Virus.

Le panneau des résultats affiche l'arborescence des ressources fichier du serveur dont les objets constitueront la couverture d'analyse.

L'arborescence des ressources fichiers du serveur contient les couvertures d'analyse prédéfinies suivantes :

- **Poste de travail**. Kaspersky Anti-Virus analyse tout le serveur.
- **Disques durs**. Kaspersky Anti-Virus analyse les objets du disque dur du serveur. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Disques amovibles**. Kaspersky Anti-Virus analyse les objets sur les disques amovibles tels que les disques compacts ou les clés USB. Vous pouvez inclure ou exclure de la couverture d'analyse tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Mémoire système**. Kaspersky Anti-Virus analyse la mémoire système et la mémoire des processus.
- **Objets exécutés au démarrage du système**. Kaspersky Anti-Virus analyse les objets sur lesquels les clés de la base de registres et les fichiers de configuration, par exemple WIN.INI ou SYSTEM.INI, s'appuient ainsi que les modules logiciels des applications qui sont exécutées automatiquement au démarrage de l'ordinateur.

- **Dossiers partagés**. Kaspersky Anti-Virus analyse tous les dossiers partagés sur le serveur protégé.
- **Emplacements réseau**. Vous pouvez ajouter à la couverture d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux répertoires de réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte **Système local** (**SYSTEM**). Pour obtenir de plus amples informations, consultez le point 9.2.1.4 à la page 129.
- **Unités virtuelles**. Vous pouvez inclure dans la couverture d'analyse les disques, les répertoires et les fichiers dynamiques ainsi que les disques montés sur le serveur, par exemple : disques partagés de la grappe (créer une *couverture d'analyse virtuelle*). Pour obtenir de plus amples informations, consultez le point 9.2.1.5 à la page 129.

Remarque

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

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

9.2.1.3. Constitution de la couverture d'analyse

Si vous administrez Kaspersky Anti-Virus sur le serveur protégé à distance via MMC, installé sur le poste de travail de l'administrateur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur.

Pour composer la couverture d'analyse :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez constituer une couverture d'analyse.

Le panneau des résultats affiche l'arborescence des ressources fichiers du serveur. Par défaut, tous les secteurs du serveur protégé seront inclus dans la couverture d'analyse.

3. Exécutez les actions suivantes :

   - pour sélectionner les nœuds que vous souhaitez inclure dans la couverture d'analyse, désélectionnez la case **Poste de travail** puis réaliser les actions suivantes :

     - Si vous souhaitez inclure tous les disques d'un même type dans la couverture d'analyse, cochez la case en regard du nom du type de disque requis ;

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

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

   - pour exclure un noeud particulier de la couverture d'analyse, déployez l'arborescence des ressources de fichiers pour afficher le noeud requis et désélectionnez la case en regard de son nom.

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

Instructions d'inclusion d'objets dans la couverture d'analyse :

- Disque de réseau, répertoire ou fichier, consultez le point 9.2.1.4 à la page 129 ;
- Disque dynamique, répertoire ou fichier, consultez le point 9.2.1.5 à la page 129.

9.2.1.4. Inclusion des disques de réseau , des répertoires ou des fichiers dans la couverture d'analyse

Vous pouvez inclure à la couverture d'analyse des disques de réseau, des répertoires ou des fichiers en indiquant leur chemin d'accès de réseau au format UNC (Universal Naming Convention).

Pour ajouter un objet de réseau à la couverture d'analyse :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dans la couverture d'analyse de laquelle vous souhaitez ajouter un chemin de réseau.
3. Ouvrez le menu contextuel au noeud **Emplacements réseau** et sélectionnez **Ajouter un répertoire de réseau** ou **Ajouter un fichier de réseau**.
4. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et enfoncez la touche **<ENTER>**.
5. Cochez la case à côté de l'objet de réseau ajouté afin de l'inclure dans la couverture d'analyse.
6. Le cas échéant, modifiez les paramètres de sécurité applicables à l'objet de réseau ajouté (cf. point 9.2.2, p. 132).
7. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

9.2.1.5. Création d'une couverture d'analyse virtuelle : inclusion des disques, répertoires et fichiers dynamiques dans la couverture d'analyse

Vous pouvez inclure dans la couverture d'analyse les disques, les répertoires et les fichiers dynamiques ainsi que les disques montés sur le serveur, par exemple : disques partagés de la grappe (créer une *couverture d'analyse virtuelle*). Pour obtenir de plus amples informations sur la couverture d'analyse virtuelle, lisez le point 6.2.1.4 à la page 76.

Vous pouvez ajouter à la couverture d'analyse virtuelle des disques, des répertoires ou des fichiers dynamiques.

Pour ajouter un disque virtuel à la couverture d'analyse :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez composer une couverture d'analyse virtuelle afin d'ouvrir la tâche.
3. Dans l'arborescence des ressources fichier du serveur du panneau des résultats, ouvrez le menu contextuel du noeud **Unités virtuelles** et dans la liste des noms disponibles, sélectionnez le nom du disque virtuel créé (cf. ill. 42).

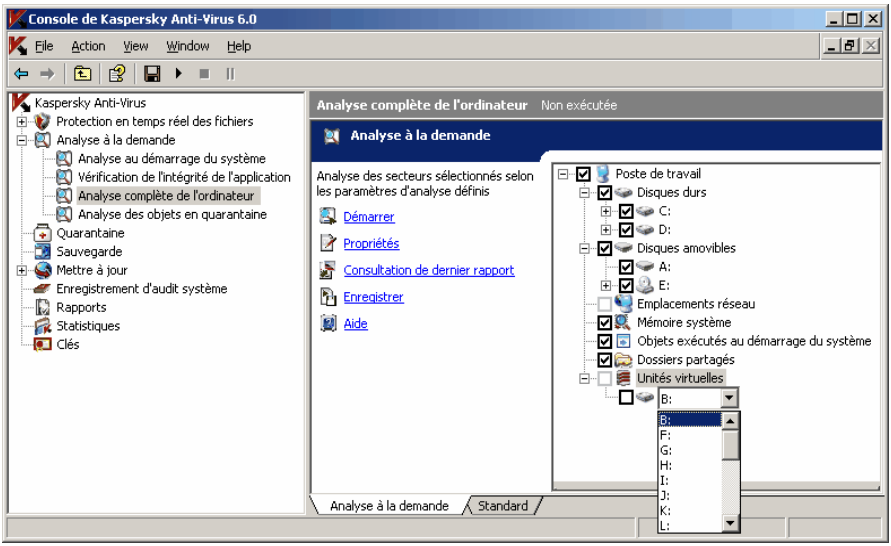

Illustration .42 Sélection du nom d'unité virtuelle créé

4. Cochez la case à côté du disque ajouté afin de l'inclure dans la couverture d'analyse.
5. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

Pour ajouter un répertoire ou un fichier virtuel dans la couverture d'analyse :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Cliquez sur la tâche d'analyse à la demande pour laquelle vous souhaitez composer une couverture d'analyse virtuelle afin d'ouvrir la tâche.
3. Accédez au panneau des résultats et dans l'arborescence des ressources fichiers du serveur ouvrez le menu contextuel du noeud auquel vous souhaitez ajouter un répertoire ou un fichier et sélectionnez **Ajouter un dossier virtuel** ou **Ajouter un fichier virtuel**.

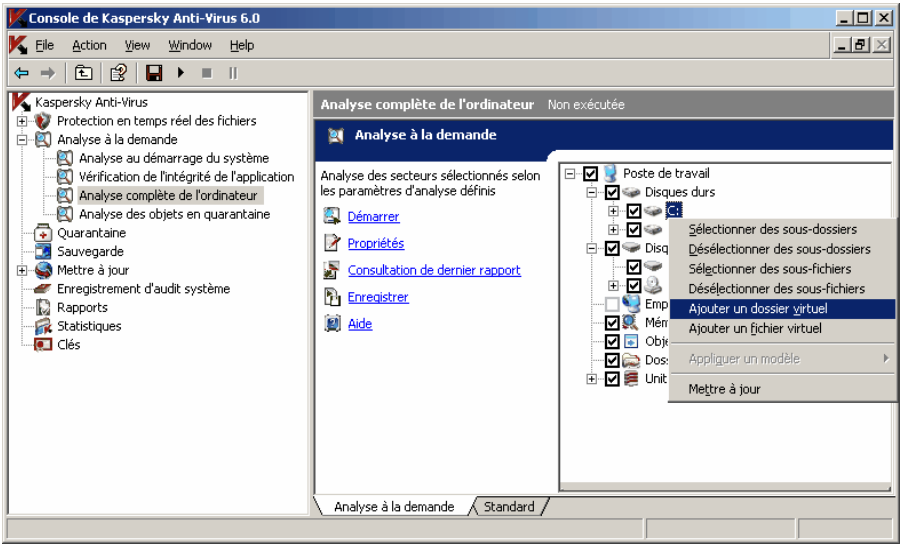

Illustration 43. Ajout d'un fichier virtuel

4. Dans le champ, saisissez le nom du répertoire (fichier). Vous pouvez définir un masque de nom de répertoire (de fichier). Pour les masques, utilisez les caractères * et ?.
5. Dans la ligne contenant le nom du répertoire (fichier) créé, cochez la case afin de l'inclure dans la couverture d'analyse.
6. Ouvrez le menu contextuel du nom de la tâche et sélectionnez la commande **Enregistrer la tâche** afin d'enregistrer les modifications dans la tâche.

9.2.2. Configuration des paramètres de sécurité pour le noeud sélectionné

Dans la tâche d'analyse à la demande sélectionnée, vous pouvez définir des paramètres de sécurité identiques pour toute la couverture d'analyse ou différents pour divers nœuds dans l'arborescence des ressources fichiers du serveur. Les paramètres de sécurité que vous définissez pour un noeud sélectionné seront automatiquement appliqué à tous les nœuds qu'il renferme. Toutefois, si vous attribuez des valeurs distinctes aux paramètres de sécurité du noeud enfant, alors les paramètres de sécurité du noeud parent ne seront pas appliqués.

Vous pouvez configurer les paramètres de la couverture d'analyse sélectionnée de l'une des manières suivantes :

- Sélectionnez un des trois niveaux de protection prédéfinis (vitesse maximale, recommandé ou protection maximum) (cf. point 9.2.2.1, p. 132) ;
- Modifier manuellement les paramètres de sécurité des nœuds sélectionnés dans l'arborescence des ressources fichier du serveur (cf. point 9.2.2.2, p. 136).

Vous pouvez enregistrer les paramètres du noeud dans un modèle afin de pouvoir l'appliquer par la suite à n'importe quel autre noeud (cf. point 9.2.2.3, p. 140).

9.2.2.1. Sélection du niveau de sécurité prédéfini dans les tâches d'analyse à la demande

Pour le noeud sélectionné dans l'arborescence des ressources fichiers du serveur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis: a) vitesse maximale, b) recommandé ou c) protection maximum. Chacun de ces niveaux prédéfinis possède sa propre sélection de paramètres de sécurité. Ces valeurs sont reprises au tableau 6.

Vitesse maximale

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

Recommandé

Le niveau de sécurité **Recommandé** est sélectionné par défaut. Les experts de Kaspersky Lab le jugent suffisant pour analyser les serveurs dans la majorité des réseaux. Ce niveau offre une combinaison idéale de qualité de l'analyse et de rapidité.

Protection maximale

Utilisez le niveau de sécurité **Protection maximale** si d'autres mesures de protection ne sont pas appliquées dans votre réseau.

Pour savoir comment configurer manuellement les paramètres de sécurité pour le noeud sélectionné dans l'arborescence des ressources fichiers, consultez le point 9.2.2 à la page 132.

Tableau 6. Niveaux de protection prédéfinis et valeurs des paramètres correspondants

Paramètres	Niveau de sécurité prédéfini		
	Vitesse maximale	**Recommandé**	**Protection maximum**
Objets à analyser (cf. point B.3.2, p. 400)	En fonction du format	Analyser tous les objets	Analyser tous les objets
Analyse uniquement des objets neufs et modifiés (cf. point B.3.3, p. 402)	Activée	Activée	Activée
Actions à exécuter sur les objets infectés (cf. point B.3.5, p. 404)	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. point B.3.6, p. 406)	Quarantaine	Quarantaine	Quarantaine
Exclusion des objets (cf. point B.3.8, p. 410)	Non	Non	Non

Paramètres	Niveau de sécurité prédéfini		
	Vitesse maximale	**Recommandé**	**Protection maximum**
Exclusion des menaces (cf. point B.3.9, p. 411)	Non	Non	Non
Durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413)	60 s	Non	Non
Taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413)	8 Mo	8 Mo	Non
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. point B.3.2, p. 400)	Oui	Oui	Oui
Analyse des secteurs d'amorçage (cf. point B.3.2, p. 400)	Oui	Oui	Oui

Paramètres	Niveau de sécurité prédéfini		
	Vitesse maximale	**Recommandé**	**Protection maximum**
Traiter les objets composés (cf. point B.3.4, p. 402)	• Archives SFX* ; • Objets compactés* ; • Objets OLE incorporés* * uniquement les objets neufs et modifiés	• Archives* ; • Archives SFX* ; • Objets compactés* ; • Objets OLE incorporés* * Tous les objets	• Archives* ; • Archives SFX* ; • Bases de données de messagerie électronique* ; • Message de texte plat* ; • Objets compactés* ; • Objets OLE incorporés* * Tous les objets

Remarque

N'oubliez pas que les paramètres de sécurité **Application de la technologie iChecker** et **Application de la technologie iSwift** ne figurent pas parmi les paramètres des niveaux prédéfinis. Ces paramètres sont désactivés par défaut. Si vous modifiez la valeur des paramètres **Application de la technologie iSwift** et **Application de la technologie iChecker**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

Pour sélectionner un des niveaux de protection prédéfinis :

1. Dans l'arborescence de la console, sélectionnez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez configurer les paramètres de sécurité.
3. Dans le panneau des résultats, sélectionnez le noeud de la couverture d'analyse auquel vous souhaitez appliquer le niveau de sécurité prédéfini.
4. Assurez-vous que ce noeud est repris dans la couverture d'analyse (cf. point 9.2.1.1 à la page 125).
5. Dans la boîte de dialogue **Niveau** (cf. ill. 44), sélectionnez le niveau que vous souhaitez appliquer.

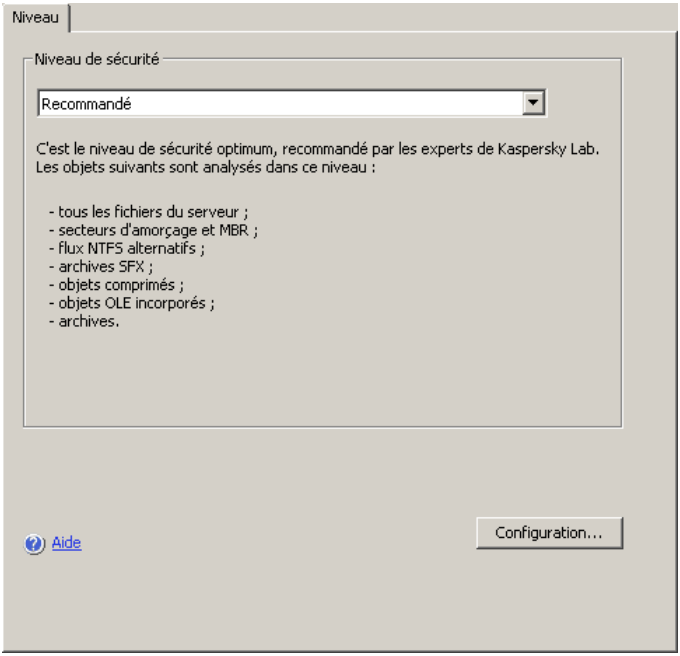

Illustration 44. Boîte de dialogue **Niveau**

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

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

9.2.2.2. Configuration manuelle des paramètres de sécurité

Pour configurer manuellement les paramètres de sécurité :

1. Dans l'arborescence de la console, sélectionnez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez configurer les paramètres de sécurité.
3. Dans le panneau des résultats, sélectionnez le noeud de la couverture d'analyse dont vous souhaitez configurer les paramètres. Assurez-vous que ce noeud est repris dans la couverture d'analyse (pour obtenir de

plus amples informations sur la couverture d'analyse, lisez le point 9.2.1.3 à la page 127).

La boîte de dialogue **Niveau** (cf. ill. 45) apparaît dans la partie inférieure du panneau des résultats.

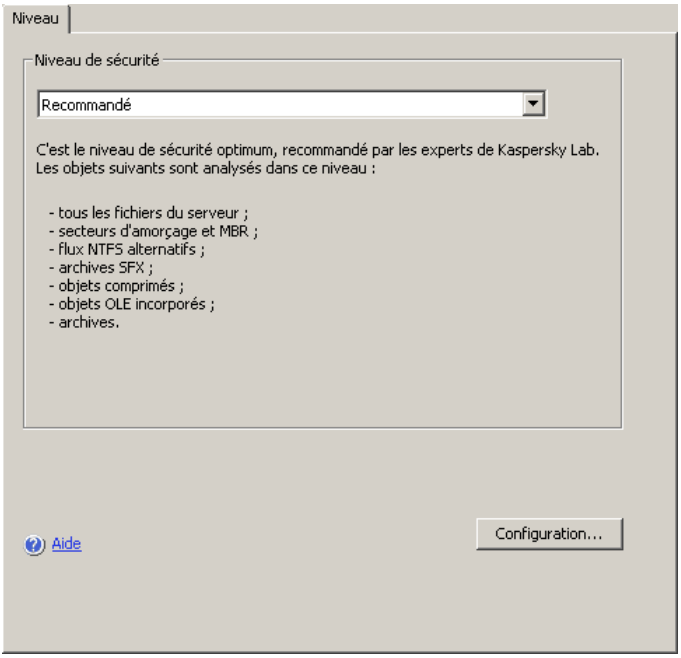

Illustration 45. Boîte de dialogue **Niveau**

Cliquez sur le bouton **Configuration** afin d'ouvrir la boîte de dialogue **Paramètres de sécurité**.

Remarque

Vous pouvez ouvrir la boîte de dialogue **Paramètres de sécurité** pour le noeud sélectionné dans l'arborescence des ressources fichiers en ouvrant le menu contextuel de ce noeud et en sélectionnant la commande **Propriétés**.

4. Dans la boîte de dialogue **Paramètres de sécurité**, configurez les paramètres requis pour le noeud sélectionné selon vos besoins.

   - Réalisez les actions suivantes sur l'onglet **Général** (cf. ill. 46) :

- Sous le titre **Couverture de l'analyse**, indiquez si Kaspersky Anti-Virus analysera tous les objets de la couverture d'analyse ou uniquement les objets d'un format ou d'une extension déterminé, si Kaspersky Anti-Virus analysera les secteurs d'amorçage des disques et l'enregistrement principal d'amorçage ou les flux NTFS alternatifs(cf. point B.3.2, p. 400) ;
- Sous le titre **Optimisation**, indiquez si Kaspersky Anti-Virus analysera tous les objets dans le secteur sélectionné ou seulement les objets neufs ou modifiés (cf. point B.3.3, p. 402) ;
- Sous le titre **Traiter les objets composés**, précisez les types d'objets composés qui seront analysés par Kaspersky Anti-Virus (cf. point B.3.4, p. 402).

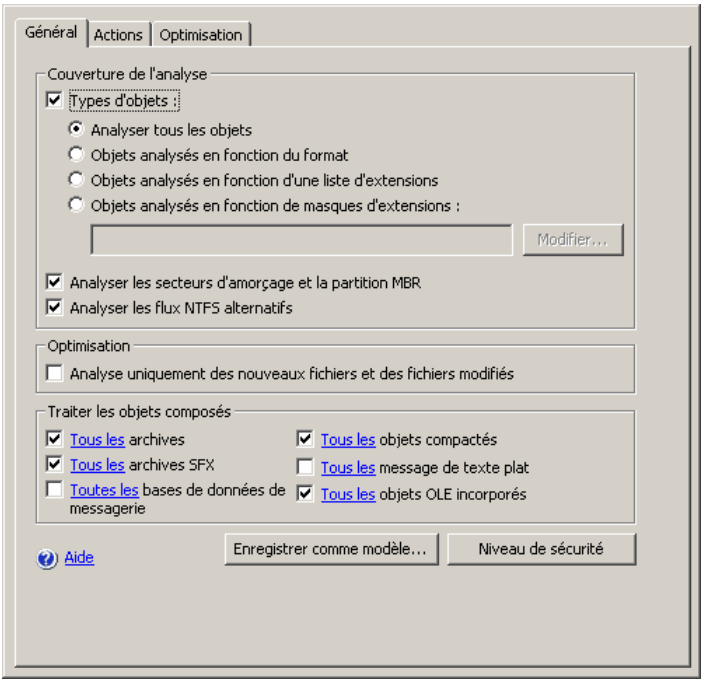

Illustration 46. Boîte de dialogue **Paramètres de sécurité** de la tâche **Analyse à la demande**, onglet **Général**

- Réalisez les actions suivantes sur l'onglet **Actions** (cf. ill. 47) :
  - Sélectionnez l'action à exécuter sur les objets infectés (cf. point B.3.5 , p. 404) ;

- Sélectionnez l'action à exécuter sur les objets suspects (cf. point B.3.6, page 406) ;
- Le cas échéant, configurez les actions à exécuter sur les objets en fonction du type de menace découverte dans ceux-ci (cf. point B.3.7, p. 408).

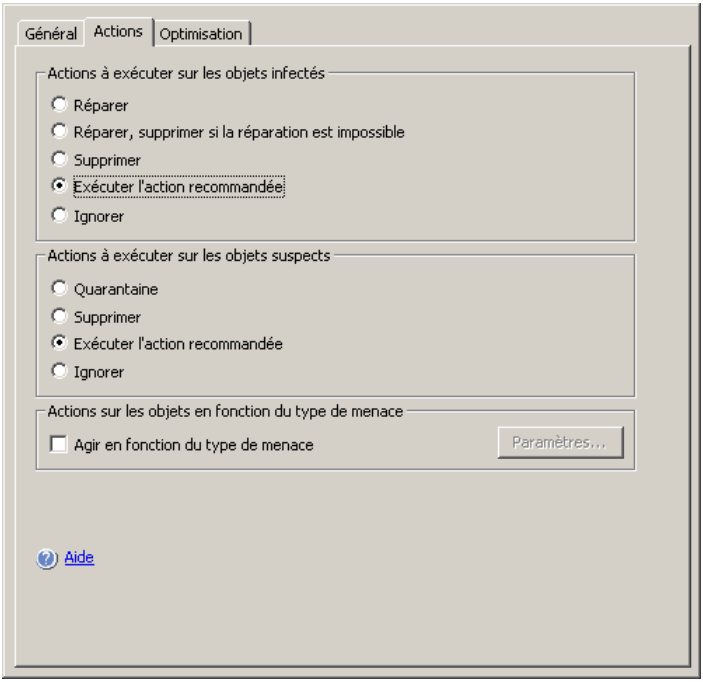

Illustration 47. Boîte de dialogue **Paramètres de sécurité** de la tâche **Analyse à la demande**, onglet **Actions**

- Réalisez les actions suivantes sur l'onglet **Optimisation** (cf. ill. 48), le cas échéant :
  - Excluez des fichiers du traitement selon le nom ou le masque (cf. point B.3.8, p. 410) ;
  - Excluez des menaces du traitement selon le nom ou le masque (cf. point B.3.9, p. 411) ;
  - Indiquez la durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413) ;
  - Précisez la taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413) ;

- Activez ou désactivez l'application de la technologie iChecker (cf. point B.3.12, p. 414) ;
- Activez ou désactivez l'application de la technologie iSwift (cf. point B.3.13, p. 415).

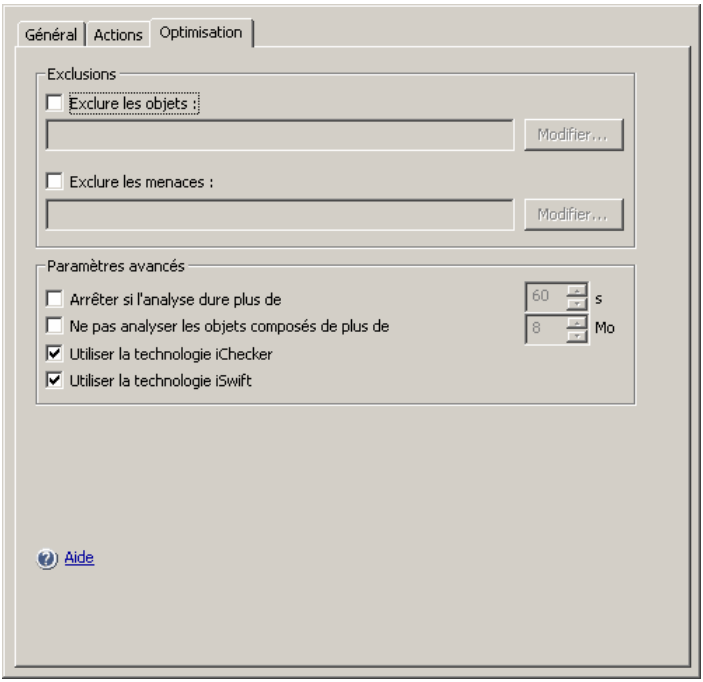

Illustration 48. Boîte de dialogue **Paramètres** de la tâche **Analyse à la demande**, onglet **Optimisation**

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

9.2.2.3. Utilisation des modèles dans les tâches d'analyse à la demande

Cette section aborde les sujets suivants :

- Enregistrement de la sélection des paramètres de sécurité dans un modèle (cf. point 9.2.2.3.1, p. 141) ;

- Consultation des paramètres de sécurité dans le modèle (cf. point 9.2.2.3.2, p. 142) ;
- Application du modèle (cf. point 9.2.2.3.3, p. 144) ;
- Suppression du modèle (cf. point 9.2.2.3.4, p. 145).

9.2.2.3.1. Enregistrement des valeurs des paramètres de sécurité dans un modèle

Après avoir configuré les paramètres de sécurité de la tâche d'analyse à la demande pour un noeud quelconque de l'arborescence des ressources fichiers du serveur, vous pouvez enregistrer ces paramètres dans un modèle afin de pouvoir les appliquer ultérieurement à d'autres nœuds de cette même tâche ou d'autres tâches de l'analyse à la demande.

Pour enregistrer l'ensemble des paramètres de sécurité dans un modèle :

1. Dans l'arborescence de la console, sélectionnez le noeud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont les paramètres doivent être enregistrés dans un modèle.
3. Dans l'arborescence des ressources fichier du réseau, sélectionnez le noeud dont vous souhaitez enregistrer les paramètres de sécurité.
4. Dans la boîte de dialogue **Paramètres de sécurité**, onglet **Général**, cliquez sur le bouton **Enregistrer dans le modèle**.
5. Réalisez les actions suivantes dans la boîte de dialogue **Propriétés du modèle** (cf. ill. 49) :
   - Dans le champ **Nom du modèle**, saisissez le nom du modèle.
   - Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.

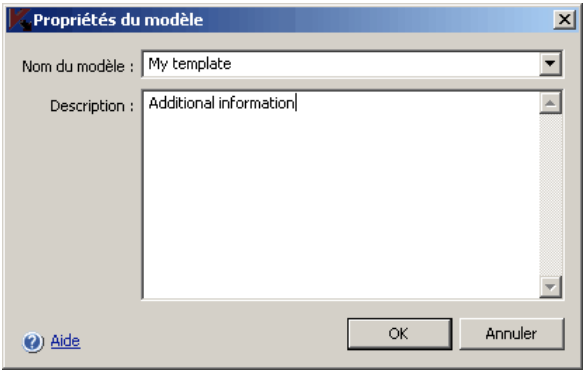

Illustration 49. Boîte de dialogue **Propriétés du modèle**

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

9.2.2.3.2. Consultation des paramètres de sécurité du modèle

Pour consulter les valeurs des paramètres de sécurité dans le modèle créé :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Analyse à la demande** et sélectionnez la commande **Modèles** (cf. ill. 50).

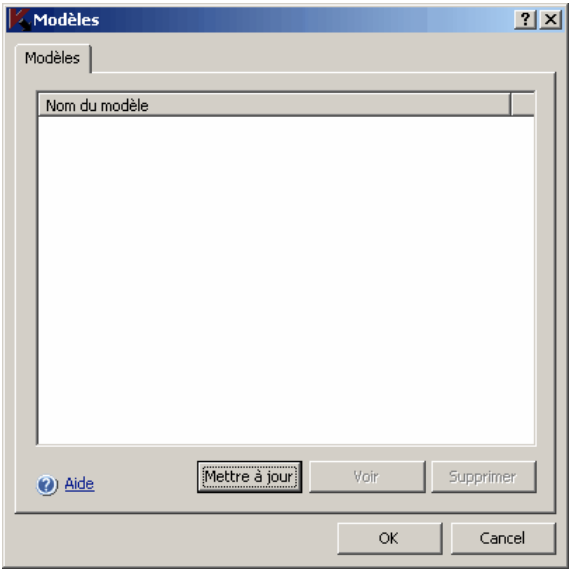

Illustration 50. Boîte de dialogue **Modèles**

Dans la boîte de dialogue **Modèles**, vous verrez la liste des modèles que vous pouvez appliquer aux tâches d'analyse à la demande.

2. Pour consulter les informations relatives au modèle et les valeurs des paramètres de sécurité qu'il contient, sélectionnez le modèle requis dans la liste et cliquez sur le bouton **Voir** (cf. ill. 51).

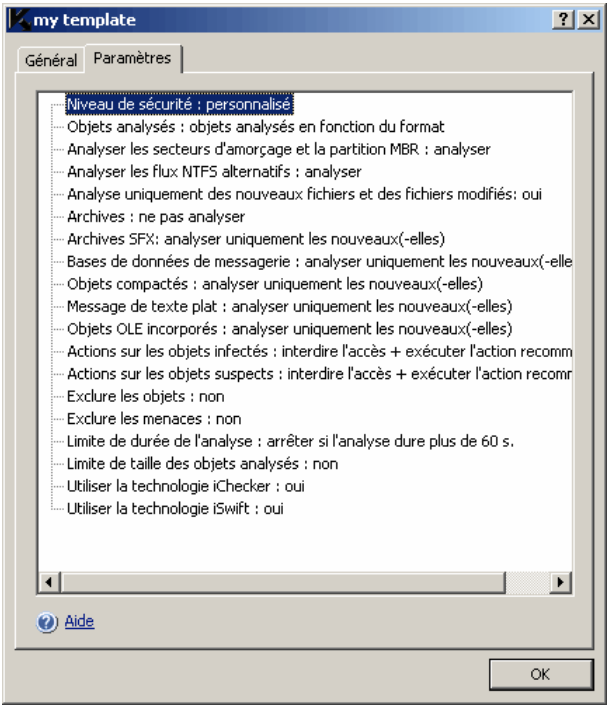

Illustration 51. Boîte de dialogue **<Nom du modèle>**, onglet **Paramètres**

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

9.2.2.3.3. Application du modèle

Pour appliquer un modèle avec les paramètres de sécurité :

1. Enregistrez tout d'abord la sélection des valeurs des paramètres de sécurité dans le modèle (cf. instructions au point 9.2.2.3.1, p. 141).
2. Dans l'arborescence de la console, sélectionnez le noeud **Analyse à la demande**.
3. Sélectionnez la tâche d'analyse à la demande à laquelle vous souhaitez appliquer les paramètres de sécurité repris dans le modèle.

4. Dans l'arborescence des ressources fichier du serveur, ouvrez le menu contextuel du menu du noeud auquel vous souhaitez appliquer le modèle et sélectionnez **Appliquer un modèle** → **Liste des modèles**.
5. Dans la liste des modèles, sélectionnez le modèle que vous souhaitez appliquer.
6. Dans la boîte de dialogue **Paramètres de sécurité**, cliquez sur **OK** afin de conserver les modifications.

Application

Si vous appliquez le modèle au nœud parent, alors les paramètres de sécurité du modèle seront appliqués à tous les nœuds enfants, sauf ceux pour lesquels vous avez configuré les paramètres de sécurité séparément.

Pour installer les paramètres de sécurité du modèle à tous les nœuds enfants, désélectionnez la case en regard du nœud parent dans l'arborescence des ressources fichier du serveur avant d'appliquer le modèle puis cochez-la à nouveau. Appliquez le modèle au nœud parent. Tous les nœuds enfants auront les mêmes paramètres de sécurité que le nœud parent.

9.2.2.3.4. Suppression du modèle

Pour supprimer un modèle :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Analyse à la demande** et sélectionnez la commande **Modèles** (cf. ill. 50).
2. Dans la boîte de dialogue **Modèles**, sélectionnez le modèle que vous souhaitez supprimer dans la liste et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**. Le modèle sélectionné sera supprimé.

9.3. Exécution en arrière-plan de la tâche d'analyse à la demande

Par défaut, les processus dans lesquels les tâches de Kaspersky Anti-Virus sont exécutées ont la priorité de base **Moyenne** (**Normal**).

Vous pouvez attribuer la priorité de base **Bas** (**Low**) au processus dans lequel la tâche d'analyse à la demande sera exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter quelques tâches en arrière-plan. Vous pouvez définir le nombre maximum de processus actifs pour les tâches en arrière plan de l'analyse à la demande (cf. point B.1.3, p. 379).

Vous pouvez définir la priorité de la tâche lors de sa création ou plus tard, dans la boîte de dialogue **Propriétés des tâches**.

Pour modifier la priorité de la tâche d'analyse à la demande :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Ouvrez le menu contextuel de la tâche d'analyse à la demande dont vous souhaitez modifier la priorité et sélectionnez la commande **Propriétés**.

   La boîte de dialogue **Propriétés de la tâche** s'ouvre (cf. ill. 52).

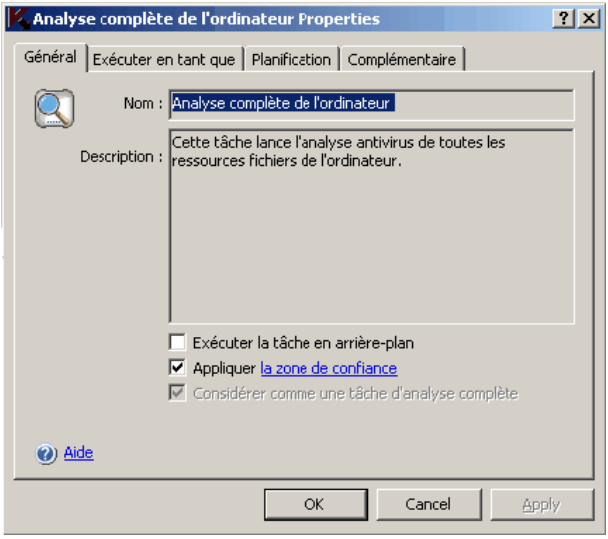

Illustration .52 Boîte de dialogue **Propriétés de la tâche**

3. Sur l'onglet **Général**, exécutez une des actions suivantes :
   - Pour activer l'exécution en arrière-plan de la tâche, cochez la case **Exécuter la tâche en arrière – plan** ;
   - Pour désactiver l'exécution en arrière-plan de la tâche, désélectionnez la case **Exécuter la tâche en arrière – plan**.

Remarque

Si vous activez ou désactivez l'exécution en arrière-plan de la tâche, la priorité de la tâche ne sera pas modifiée immédiatement mais uniquement au prochain lancement.

9.4. Statistiques des tâches d'analyse à la demande

Pendant que la tâche d'analyse à la demande est exécutée, vous pouvez consulter des informations détaillées sur le nombre d'objets traités par Kaspersky Anti-Virus depuis son lancement jusqu'à maintenant dans la boîte de dialogue **Statistiques**.

Les informations de la boîte de dialogue **Statistiques** sont accessibles lorsque la tâche est suspendue. Après la fin ou la suspension de la tâche, vous pouvez consulter ces informations dans le rapport détaillé sur les événements survenus dans la tâche (cf. point 13.2.4, p. 211).

Pour consulter les statistiques d'une tâche d'analyse à la demande :

1. Dans l'arborescence de la console, développez le noeud **Analyse à la demande**.
2. Ouvrez le menu contextuel de la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques et sélectionnez la commande **Voir les statistiques** (cf. ill. 53).

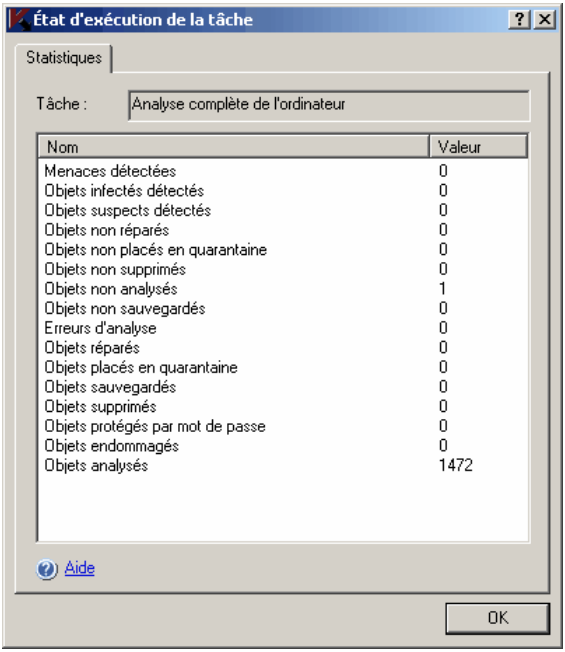

Illustration 53. Boîte de dialogue **Etat d'exécution de la tâche**

Dans la boîte de dialogue **Etat d'exécution de la tâche**, vous pourrez consulter les informations suivantes sur les objets traités par Kaspersky Anti-Virus depuis son lancement jusque maintenant :

- Dans la tâche **Analyse de l'intégrité de l'application** :

Champ	Description
Modules dont l'intégrité a été violée	Nombre de modules dont l'intégrité a été violée. Si des modules dont l'intégrité a été violée sont identifiés, procédez à la restauration de Kaspersky Anti-Virus. Consultez les instructions du document *Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition. Manuel d'installation.*
Modules analysés	Nombre total de modules analysés.

- Dans les tâches **Analyse complète de l'ordinateur**, **Analyse au démarrage du système**, **Analyse des objets en quarantaine** et dans les tâches d'analyse à la demande définies par l'utilisateur :

Champ	Description
Menaces détectées	Nombre de menaces détectées ; par exemple, si Kaspersky Anti-Virus a découvert un programme malveillant dans cinq objets, la valeur de ce champ augmentera d'une unité.
Objets infectés détectés	Nombre total d'objets infectés découverts.
Objets suspects détectés	Nombre total d'objets suspects découverts.
Objets non-réparés	Nombre d'objets que Kaspersky Anti-Virus n'a pas réparé parce que : a) le type de menace de l'objet ne peut être réparé la réparation, b) les objets de ce type ne peuvent pas être réparés ou c) une erreur s'est produite durant.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Anti-Virus aurait du mettre en quarantaine mais sans réussir à cause d'une erreur tel que le manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Anti-Virus a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone d'analyse que Kaspersky Anti-Virus n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par un autre programme.
Objets non sauvegardés	Nombre de fichiers dont les copies auraient du être placées par Kaspersky Anti-Virus en sauvegarde mais qui n'ont pas pu l'être en raison d'une erreur.
Erreurs d'analyse	Nombre d'objets dont le traitement a entraîné une erreur de Kaspersky Anti-Virus.
Objets réparés	Nombre d'objets réparés par Kaspersky Anti-Virus.

Champ	Description
Placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Anti-Virus.
Objets sauvegardés	Nombre d'objets dont une copie a été mise en sauvegarde par Kaspersky Anti-Virus.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Anti-Virus.
Objets protégés par mot de passe	Nombre d'objets (par exemple, archives) que Kaspersky Anti-Virus a ignoré car ils étaient protégés par un mot de passe.
Objets endommagés	Nombre d'objets ignorés par Kaspersky Anti-Virus car leur format était corrompu.
Objets analysés	Nombre total d'objets analysés par Kaspersky Anti-Virus.

CHAPITRE 10. MISE A JOUR DES BASE ET DES MODULES LOGICIELS DE KASPERSKY ANTI-VIRUS

Cette section aborde les sujets suivants :

- Présentation de la mise à jour des bases de Kaspersky Anti-Virus (cf. point 10.1, p. 152) ;
- Présentation de la mise à jour des modules logiciels (cf. point 10.2, p. 153) ;
- Schémas de mise à jour des bases et des modules logiciels des applications antivirus dans l'entreprise (cf. point 10.3, p. 154) ;
- Description des tâches de mise à jour (cf. point 10.4, p. 158) ;
- Configuration des tâches liées à la mise à jour :
  - Sélection de la source des mises à jour, configuration de la connexion à la source des mises à jour, définition de l'emplacement du serveur protégés dans les tâches de mise à jour (cf. point 10.5.1, p. 160) ;
  - Configuration des paramètres de la tâche *Mise à jour des modules de l'application* (cf. point 10.5.2, p. 165) ;
  - Configuration des paramètres de la tâche *Copie des mises à jour* (cf. point 10.5.3, p. 167) ;
- Statistiques des tâches de mise à jour (cf. point 10.6, p. 169) ;
- Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus (cf. point 10.7, p. 170) ;
- Remise à l'état antérieur à la mise à jour des modules logiciels (cf. point 10.8, p. 170).

10.1. Présentation de la mise à jour des bases de Kaspersky Anti-Virus

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

Par défaut, si les bases de Kaspersky Anti-Virus ne sont pas actualisées dans la semaine qui suit la création des dernières mises à jour des bases installées, l'événement *Les bases sont dépassées* est déclenché et si les bases ne sont pas actualisées dans les deux semaines, l'événement *Les bases de données sont périmées* s'affiche (les informations sur l'actualité des bases apparaissent dans le noeud **Statistiques,** cf. point 13.4 à la page 224). Vous pouvez définir un nombre de jours différents avant le déclenchement de ces deux événements à l'aide des paramètres généraux de Kaspersky Anti-Virus (cf. point 3.2, p. 46) ainsi que configurer les notifications des administrateurs sur ces événements (cf. point 15.2, p. 238).

Vous pouvez actualiser les bases depuis les *serveurs de mise à jour* FTP ou HTTP de Kaspersky Lab ou depuis n'importe quelle autre source de mises à jour grâce à la tâche **Mise à jour des bases** de Kaspersky Anti-Virus. Pour obtenir de plus amples informations sur la tâche **Mise à jour des tâches**, lisez le point 10.4 à la page 158.

Vous pouvez télécharger les mises à jour sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les serveurs. Si vous utilisez Kaspersky Administration Kit pour l'administration centralisée de la protection des ordinateurs de l'entreprise, vous pouvez utiliser le serveur d'administration de Kaspersky Administration Kit en guise d'intermédiaire pour le chargement des mises à jour. Pour copier les bases sur l'ordinateur intermédiaire sans les appliquer, utilisez la tâche **Copie des mises à jour**. Pour obtenir de plus amples informations sur cette tâche, lisez le point 10.4 à la page 158.

Vous pouvez lancer les tâches de mise à jour manuellement ou selon un programme (pour en savoir plus sur la programmation de la tâche, consultez le point 5.7 à la page 60).

Si le chargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Anti-Virus reviendra automatiquement à l'utilisation des dernières mises à jour installées. En cas de corruption des bases de Kaspersky Anti-Virus, vous pouvez vous-même *revenir à l'état antérieur* à l'installation des mises à jour (cf. point 10.7, p. 170).

Remarque

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

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

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

Les mises à jour urgentes sont publiées sur les serveurs de mise à jour de Kaspersky Lab. Vous pouvez les charger et les installer automatiquement via la tâche **Mise à jour des modules de l'application**.

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

Vous pouvez télécharger les mises à jour urgentes depuis Internet sur chaque serveur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez les mises à jour sans les installer avant de la diffuser sur les serveurs. Pour copier et enregistrer les mises à jour sans les installer, utilisez la tâche **Copie des mises à jour**. Pour obtenir de plus amples informations sur cette tâche, lisez le point 10.4 à la page 158.

Avant d'installer les mises à jour des modules logiciels, Kaspersky Anti-Virus crée une copie de sauvegarde des modules installés antérieurement. Si la mise à jour des modules logiciels est interrompue ou si elle se solde par un échec, Kaspersky Anti-Virus utilisera automatiquement les modules logiciels installés précédemment. Vous pouvez également *revenir manuellement à l'état antérieur à la mise à jour des modules logiciels* (cf. point 10.8, p. 170).

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

Remarque

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

10.3. Schémas de mise à jour des bases et des modules logiciels des applications antivirus dans l'entreprise

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

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

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

  Le rôle d'ordinateur intermédiaire peut être rempli par n'importe que ordinateur doté de :

  - Kaspersky Anti-Virus (un des serveurs protégés) (**schéma 2)**

ou

- Serveur d'administration Kaspersky Administration Kit (**schéma 3**).

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

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

Schéma 1. Mise à jour directement depuis Internet

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

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

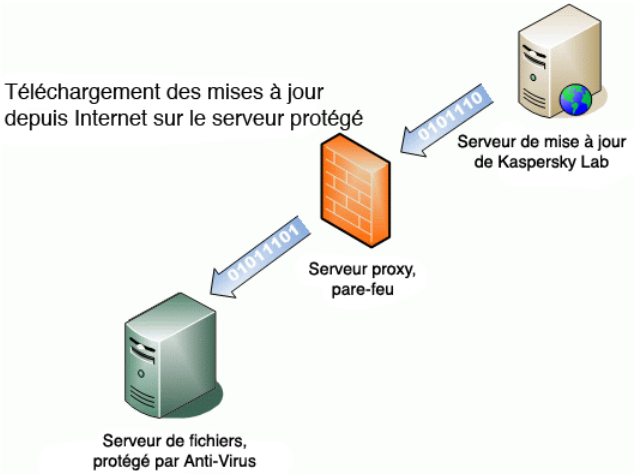

Illustration 54. Mise à jour directement depuis Internet

Schéma 2. Mise à jour via un des serveurs protégés

La mise à jour dans ce cas (cf. ill. 55) comporte les étapes suivantes :

Etape 1. Téléchargement des mises à jour depuis Internet vers l'ordinateur intermédiaire sélectionné par l'utilisateur

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

A l'aide de cette tâche, vous pouvez également obtenir les mises à jour non seulement pour les serveurs protégés mais également pour les ordinateurs du réseau local sur lesquels sont installées d'autres applications de Kaspersky Lab version 6.0 (par exemple, Kaspersky Anti-Virus 6.0 for Windows Workstations).

Etape 2. Copie des mises à jour de l'ordinateur intermédiaire les serveurs protégés

Sur chacun des serveurs protégés, configurez la tâche **Mise à jour des bases de l'application** (**Mise à jour des modules de l'application**). En guise de source des mises à jour pour cette tâche, saisissez le répertoire de l'ordinateur intermédiaire dans lequel vous avez copié les mises à jour.

Illustration 55. Mise à jour via un des serveurs protégés

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

Si vous utilisez l'application Kaspersky Administration Kit pour assurer l'administration centralisée de la protection de l'ordinateur, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Administration Kit (cf. ill. 56).

Illustration 56. Mise à jour par le serveur d'administration Kaspersky Administration Kit.

La mise à jour dans ce cas comporte les étapes suivantes :

Etape1. Téléchargement des mises à jour depuis Internet vers le serveur d'administration Kaspersky Administration Kit

Configurez la tâche globale **Récupération des mises à jour par le serveur d'administration**. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.

Vous pouvez obtenir les mises à jour non seulement pour les serveurs protégés mais également pour les autres ordinateurs du réseau local sur lesquels sont installées d'autres applications de Kaspersky Lab version 6.0 (par exemple, Kaspersky Anti-Virus 6.0 for Windows Workstations).

Etape 2. Copie des mises à jour du serveur d'administration Kaspersky Administration Kit sur les serveurs protégés

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

- Configurez sur le serveur d'administration Kaspersky Administration Kit une tâche de groupe de mise à jour des bases (des modules) de Kaspersky Anti-Virus afin de diffuser les mises à jour vers les serveurs protégés ; dans la programmation de la tâche, attribuez la valeur **A la ré-**

ception des mises à jour par le serveur d'administration à la fréquence d'exécution. Le serveur d'administration exécutera la tâche chaque fois qu'il reçoit les mises à jour (cette méthode est la méthode recommandée).

Programmez l'exécution de la tâche. Pour une tâche créée dans la console d'administration, vous pouvez attribuer la valeur **Après réception des mises à jour par le serveur d'administration** à la fréquence d'exécution. La tâche sera exécutée chaque fois que le serveur d'administration recevra la mise à jour des bases.

Remarque

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

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

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

10.4. Tâches de mise à jour

Kaspersky Anti-Virus prévoit quatre tâches prédéfinies de mise à jour : **Mise à jour des bases de l'application**, **Mises à jour des modules de l'application**, **Copie des mises à jour** et **Annulation de la mise à jour** (cf. ill. 57).

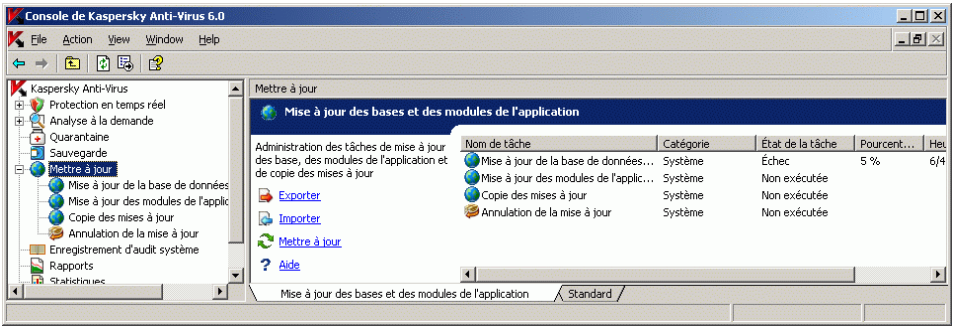

Illustration 57. Tâches de mise à jour dans la fenêtre de la console de Kaspersky Anti-Virus

Mise à jour des bases de l'application

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

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

Mise à jour des modules de l'application

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

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

Copie des mises à jour

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

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

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

Pour en savoir plus sur la configuration de la tâche de mise à jour, consultez le point 10.5 à la page 160.

Remarque

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

Pour savoir comment administrer les tâches dans Kaspersky Anti-Virus, consultez le point 5.6, page 60.

10.5. Configuration des tâches liées à la mise à jour

Cette section décrit comment réaliser les actions suivantes dans les tâches de mise à jour :

- Sélectionner la source des mises à jour, configurer la connexion à la source des mises à jour, définir l'emplacement du serveur protégé pour optimiser la réception des mises à jour (ces paramètres figurent dans chaque tâche de mise à jour) (cf. point 10.5.1, p. 160) ;
- Configurer les paramètres de la tâche *Mise à jour des modules de l'application* (cf. point 10.5.2, p. 165) ;
- Configurer les paramètres de la tâche *Copie des mises à jour* (cf. point 10.5.3, p. 167).

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

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

Pour configurer les paramètres de la mise à jour :

1. Dans l'arborescence de la console, sélectionnez **Mise à jour**.

2. Ouvrez le menu contextuel de la tâche de mise à jour pour laquelle vous souhaitez configurer la source et sélectionnez **Propriétés**.

   Dans les onglets de la boîte de dialogue **Propriétés de la tâche**, définissez les paramètres de mise à jour en fonction de vos besoins.

3. Sur l'onglet **Général** (cf. ill. 58), sélectionnez la source d'où vous souhaitez recevoir la mise à jour (pour de plus amples informations sur ce paramètre, consultez le point B.5.1, page 423).

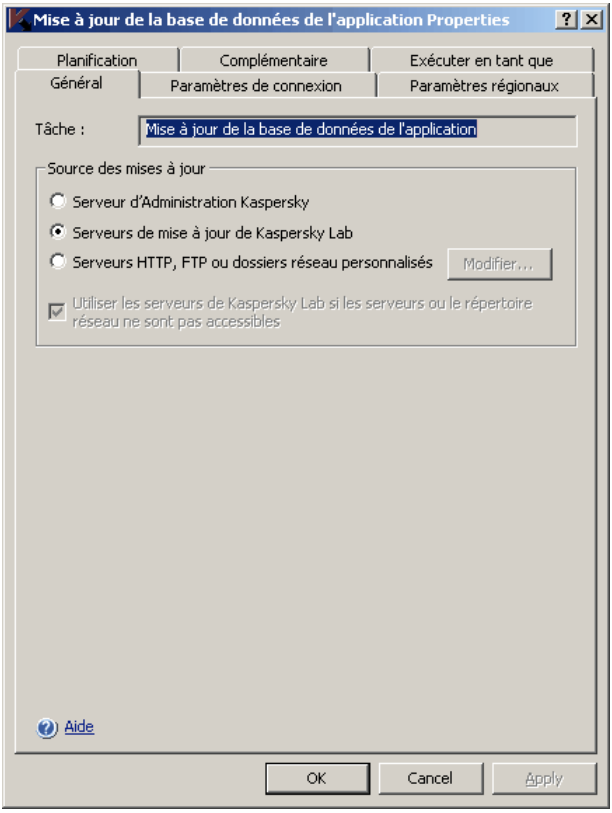

Illustration 58. Boîte de dialogue **Propriétés de la tâche**, onglet **Général**

4. Si vous avez choisi l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés**, ajoutez un ou plusieurs sources de mises à jour définies par l'utilisateur. Pour indiquer la source, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Serveurs de mises à jour** (cf. ill. 59), cliquez sur le bouton **Ajouter** et dans le champ, saisissez l'adresse du répertoire contenant les fichiers de la mise à jour sur le

serveur FTP ou HTTP ; saisissez le répertoire local ou de réseau au format UNC (Universal Naming Convention). Cliquez sur **OK**.

Vous pouvez activer ou désactiver les sources ajoutées par l'utilisateur : pour désactiver une source, désélectionnez la case en regard de son nom dans la liste ; pour activer une source, cochez la case en regard de son nom dans la liste.

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

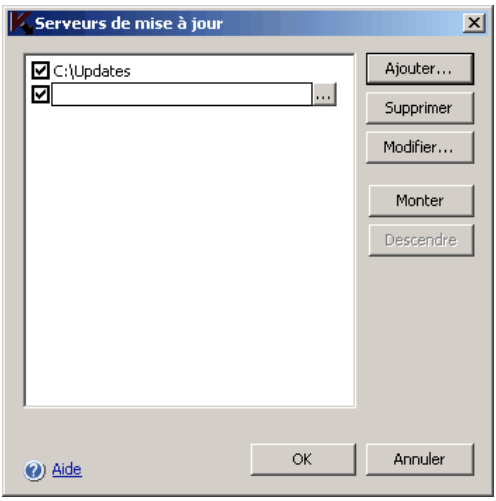

Illustration 59. Ajout de sources de mise à jour définies par l'utilisateur

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

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

5. Pour utiliser les serveurs de mise à jour de Kaspersky Lab afin de recevoir les mises à jour au cas où les sources définies par l'utilisateur seraient inaccessibles, cochez la case **Utiliser les serveurs de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles**.

6. Sur l'onglet **Paramètres de connexion** (cf. ill. 60), configurez la connexion à la source des mises à jour.

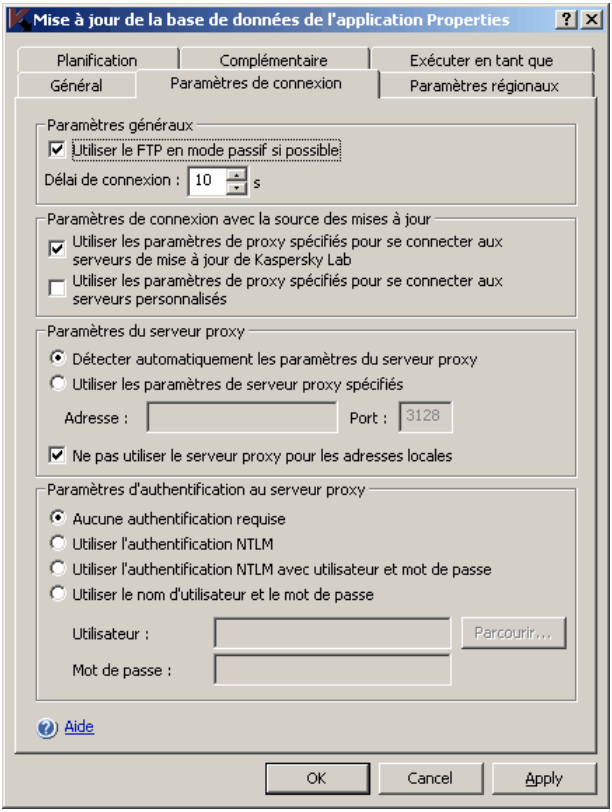

Illustration 60. Onglet **Paramètres de connexion**

Exécutez les actions suivantes :

- Indiquez le mode du serveur FTP pour la connexion au serveur protégé (cf. point B.5.2, p. 424) ;
- Le cas échéant, modifiez le délai d'attente pour la connexion à la source des mises à jour (cf. point B.5.3, p. 425) ;
- Si la réception des mises à jour depuis une des sources indiquées requiert l'accès au serveur proxy, décrivez les paramètres d'accès à ce dernier :
  - Requête adressée au serveur proxy lors de la connexion à diverses sources de mises à jour (cf. point B.5.4.1, p. 426) ;
  - Adresse du serveur proxy (cf. point B.5.4.2, p. 427) ;

- Méthode de vérification de l'authenticité lors de l'accès au serveur proxy (cf. point B.5.4.3, p. 428).

7. Sur l'onglet **Paramètres régionaux** (cf. ill. 61), sélectionnez le pays où se trouve le serveur protégé dans la liste **Emplacement** (pour de plus amples informations sur ce paramètre, consultez le point B.5.5, page 429).

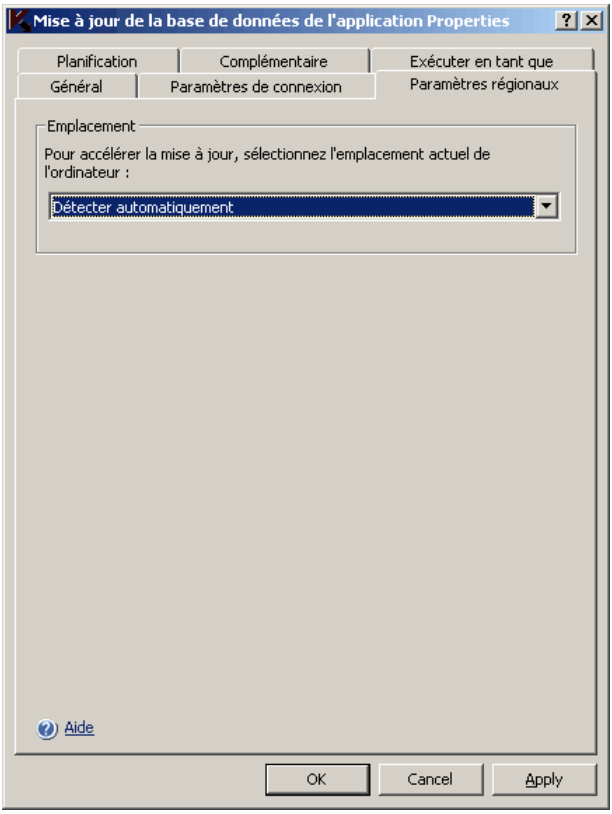

Illustration 61. Boîte de dialogue **Paramètres de mise à jour**, onglet **Paramètres régionaux**

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

10.5.2. Configuration des paramètres de la tâche *Mise à jour des modules de l'application*

Pour configurer les paramètres de la tâche ***Mise à jour des modules de l'application*** *:*

1. Dans l'arborescence de la console, sélectionnez le noeud **Mise à jour**.
2. Ouvrez le menu contextuel de la tâche **Mise à jour des modules de l'application** et sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés: Mise à jour des modules de l'application**, définissez la source des mises à jour et les paramètres de connexion à celle-ci (cf. les instructions du point 10.5.1 à la page 160).
4. Sur l'onglet **Général** (cf. ill 62), décidez s'il faut copier et installer les mises à jour ou uniquement vérifier si elle sont présentes (pour de plus amples informations sur ce paramètre, consultez le point B.5.6.1 à la page 431).

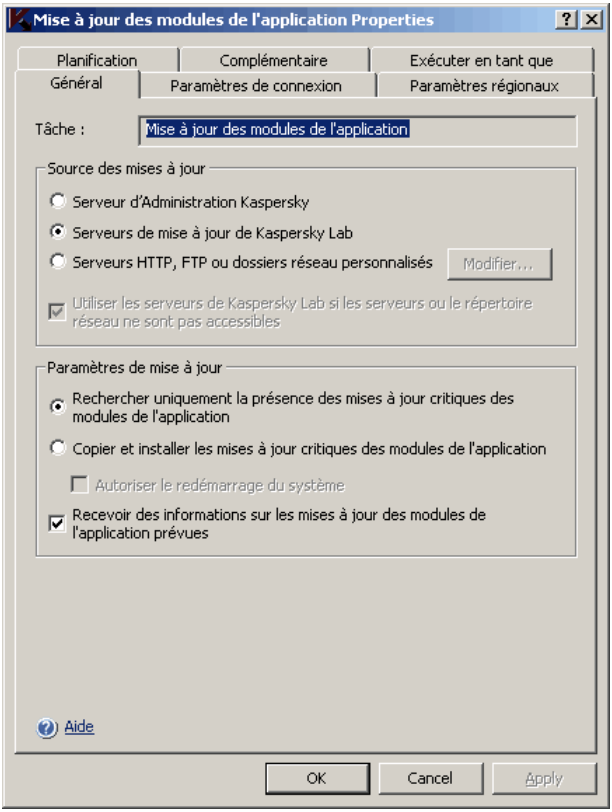

Illustration 62. Boîte de dialogue **Propriétés: Mise à jour des modules de l'application**, onglet **Général**

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

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

   Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez configurer les notifications adressées à l'administrateur pour l'événement

Des mises à jour prévues des modules de Kaspersky Anti-Virus sont disponibles. Cette notification reprend l'adresse des pages de notre site d'où les mises à jour prévues pourront être téléchargées (pour de plus amples informations sur la configuration des notifications, consultez le point 15.2 à la page 238).

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

10.5.3. Configuration des paramètres de la tâche *Copie des mises à jour*

*Pour configurer les paramètres de la tâche **Copie des mises à jour** :*

1. Dans l'arborescence de la console, sélectionnez le noeud **Mise à jour**.
2. Ouvrez le menu contextuel de la tâche **Copie des mises à jour** et sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés: Copie des mises à jour**, définissez la source des mises à jour et les paramètres de connexion à celle-ci (cf. les instructions du point 10.5.1 à la page 160).

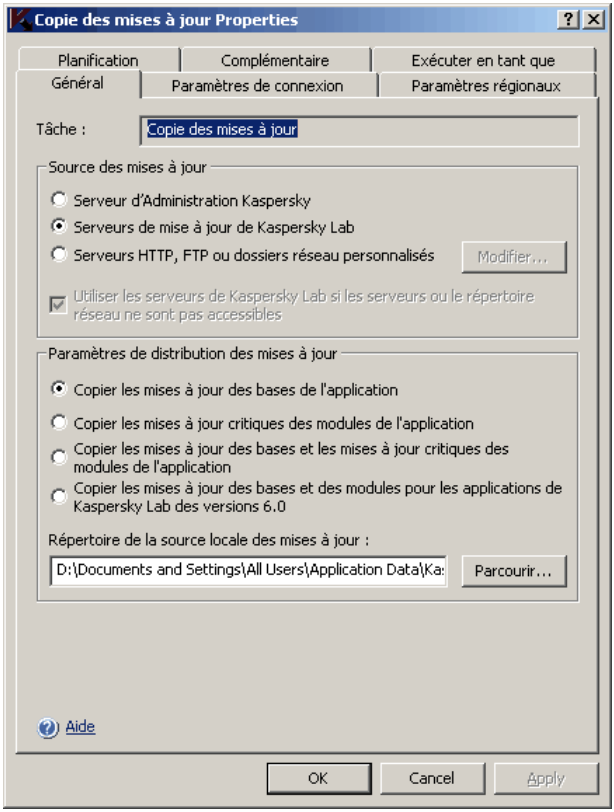

Illustration 63. Boîte de dialogue **Propriétés: Copie des mises à jour**, onglet **Général**

4. Dans l'onglet **Général**, définissez la composition des mises à jour qui seront copiées dans le répertoire indiquée (pour de plus amples informations sur le paramètre, consultez le point B.5.7.1 à la page 432).
5. Indiquez le répertoire local ou de réseau dans lequel Kaspersky Anti-Virus conservera les mises à jour téléchargées (pour de plus amples informations sur le paramètre, consultez le point B.5.7.2 à la page 434).
6. Cliquez sur **OK** pour enregistrer les modifications.

10.6. Statistiques des tâches de mise à jour

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

Les informations de la boîte de dialogue **Statistiques** sont accessibles lorsque la tâche est suspendue. Après la fin ou la suspension de la tâche, vous pouvez consulter ces informations dans le rapport détaillé sur les événements survenus dans la tâche (cf. point 13.2.4, p. 211).

Pour consulter les statistiques de la tâche de mise à jour :

1. Dans l'arborescence de la console, déployez le noeud **Mise à jour**.
2. Ouvrez le menu contextuel de la tâche requise et sélectionnez **Voir les statistiques**.

Dans la boîte de dialogue **Etat de l'exécution de la tâche** des tâches **Mise à jour des bases de l'application** et **Copie des mises à jour** vous pourrez voir les informations relatives au volume de données téléchargées par Kaspersky Anti-Virus en ce moment (**Données téléchargées**).

La boîte de dialogue **Etat d'exécution de la tâche Mise à jour des modules de l'application** reprend les informations suivantes :

Champ	Description
Données téléchargées	Volume totale de données téléchargées.
Mises à jour prévues disponibles	Nombre de mises à jour prévues prêtes pour l'installation.
Mises à jour critiques disponibles	Nombre de mises à jour critiques disponibles pour l'installation.
Erreur d'application des mises à jour	Si la valeur de ce champ est différente de zéro, la mise à jour n'a pas été appliquée. Le rapport détaillé sur l'exécution des tâches reprend le nom des mises à jour dont l'application a entraîné une erreur.

10.7. Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus

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

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

10.8. Remise à l'état antérieur à la mise à jour des modules logiciels

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

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

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

CHAPITRE 11. ISOLEMENT DES OBJETS SUSPECTS. UTILISATION DE LA QUARANTAINE

Le présent chapitre aborde les sujets suivants :

- Présentation de l'isolement des objets suspects (cf. point 11.1, p. 171) ;
- Consultation des objets en quarantaine, tri et filtrage des objets (cf. point 11.2, p. 172) ;
- Analyse des objets en quarantaine (à la demande ou automatiquement après chaque mise à jour des bases (cf. point 11.3, p. 177) ;
- Restauration des objets en quarantaine (cf. point 11.4, p. 179) ;
- Mise en quarantaine manuelle des objets (cf. point 11.5, p. 183) ;
- Suppression des objets en quarantaine (cf. point 11.6, p. 184) ;
- Envoi des objets suspects de la quarantaine à Kaspersky Lab pour examen (cf. 11.7, p. 184) ;
- Configuration des paramètres de la quarantaine (cf. point 11.8, p. 186) ;
- Statistiques de la quarantaine (cf. point 11.9, p. 188).

Les paramètres de la quarantaine sont décrits au point B.6 à la page 434.

11.1. Présentation de l'isolement des objets suspects

Kaspersky Anti-Virus isole les objets qu'il estime suspects et les met en *quarantaine* : il les déplace de l'emplacement d'origine vers un répertoire spécial dans lequel ils seront cryptés pour des raisons de sécurité (pour de plus amples informations sur la manière dont Kaspersky Anti-Virus reconnaît les objets suspects, lisez le point 1.1.3 à la page 20).

11.2. Consultation des objets en quarantaine

Vous pouvez consulter les objets en quarantaine dans le noeud **Quarantaine** de la console de Kaspersky Anti-Virus.

*Pour consulter les objets en quarantaine, sélectionnez le noeud **Quarantaine** (cf. ill. 64) dans l'arborescence de la console.*

Pour trouver l'objet requis dans la liste des objets en quarantaine, vous pouvez les trier (cf. point 11.2.1, 175) ou les filtrer (11.2.2, p. 175).

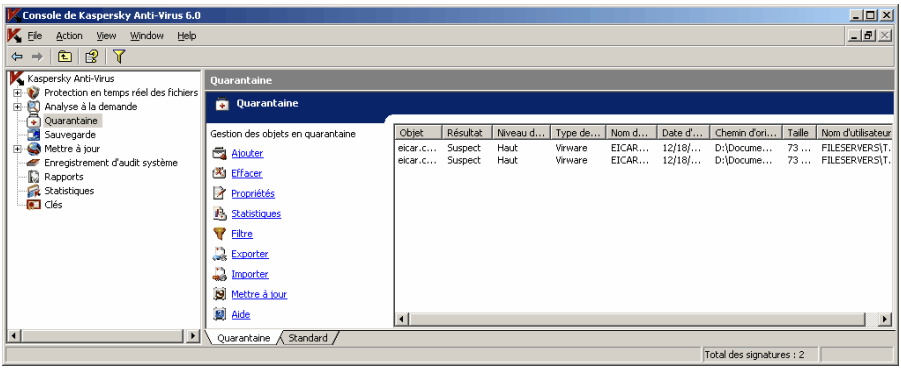

Illustration 64. Informations relatives aux objets en quarantaine dans le noeud **Quarantaine**

Le panneau des résultats reprend les informations suivantes pour chaque objet en quarantaine :

Tableau 7. Information sur les objets en quarantaine

Champ	Description
Objet	Nom de l'objet placé en quarantaine

Champ	Description
Résultat	Etat de l'objet en quarantaine, peut prendre les valeurs suivantes : • **Avertissement**. L'analyseur heuristique considère cet objet comme un objet suspect ; • **Suspect**. L'objet est suspect ; il existe une équivalence partielle entre une partie du code de l'objet et une partie du code d'une menace connue ; • **Infecté**. L'objet est suspect ; il existe une équivalence parfaite entre une partie du code de l'objet et une partie du code d'une menace connue ; • **Fausse alerte**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est sain. • **Réparé**. Kaspersky Anti-Virus a placé l'objet en quarantaine en tant qu'objet suspect ou vous avez mis l'objet manuellement en quarantaine mais l'analyse de la quarantaine à l'aide des bases actualisées de Kaspersky Anti-Virus indique que l'objet est infecté mais qu'il a pu être réparé. Vous pouvez restaurer l'objet sans craintes ; • **Ajouté par l'utilisateur**. L'objet a été placé en quarantaine par l'utilisateur.

Champ	Description
Niveau de danger	Le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace présente dans l'objet et il peut prendre une des valeurs suivantes (pour en savoir plus sur les types de menaces, consultez le point 1.1.2 à la page 14) : • **Haut**. L'objet contient une menace de type *vers de réseau*, *virus traditionnels*, *chevaux de Troie* ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues) ; • **Moyen**. L'objet peut contenir une menace du type *autres programmes malveillants*, *logiciels publicitaires* ou *programmes au contenu pornographique* ; • **Bas**. L'objet peut contenir une menace du type *programmes présentant un risque potentiel* ; • **Pour information**. L'objet a été placé en quarantaine par l'utilisateur.
Type de menace	Type de menaces selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté.
Nom de menace	Nom de menace selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace dans l'objet donné par Kaspersky Anti-Virus lorsqu'il a identifié un objet comme étant suspect ou infecté. Vous pouvez obtenir le nom complet de la menace découverte dans l'objet dans le rapport détaillé de l'exécution de la tâche. (noeud **Rapports**).
Date de placement	Date de placement de l'objet en quarantaine.
Chemin d'origine	Chemin d'accès complet à l'emplacement d'origine de l'objet, par exemple au répertoire où se trouvait l'objet avant d'être placé en quarantaine, au fichier dans l'archive ou au fichier *pst* de la base de messagerie.
Taille	Taille de l'objet.

Champ	Description
Nom d'utilisateur	Cette colonne affiche les données suivantes : • Si l'objet a été isolé par Kaspersky Anti-Virus dans la tâche **Protection en temps réel des fichiers** – le nom du compte utilisateur sous les privilèges duquel l'application a sollicité l'objet au moment de l'interception ; • Si l'objet a été isolé par Kaspersky Anti-Virus dans la tâche d'analyse à la demande – le nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée ; • Si l'utilisateur a placé l'objet en quarantaine manuellement – le nom du compte de cet utilisateur.

11.2.1. Tri des objets en quarantaine

Par défaut, les objets dans la liste des objets en quarantaine sont triés par date de placement dans l'ordre chronologique inverse. Pour trouver l'objet souhaité, vous pouvez trier la liste selon le contenu des colonnes reprenant les informations sur les objets. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Quarantaine**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour trier les objets :

1. Dans l'arborescence de la console, sélectionnez le noeud **Quarantaine**.
2. Dans le panneau des résultats, cliquez sur le titre de la colonne selon laquelle vous souhaitez trier les objets de la liste.

11.2.2. Filtrage des objets en quarantaine

Pour trouver l'objet souhaité en quarantaine, vous pouvez filtrer les objets de la liste et afficher uniquement ceux qui répondent aux critères de filtrage que vous avez définis. Les résultats du filtrage sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Quarantaine**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour définir un ou plusieurs filtres :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Quarantaine** et sélectionnez **Filtre**.

   La boîte de dialogue **Paramètres du filtre** s'ouvre (cf. ill. 65).

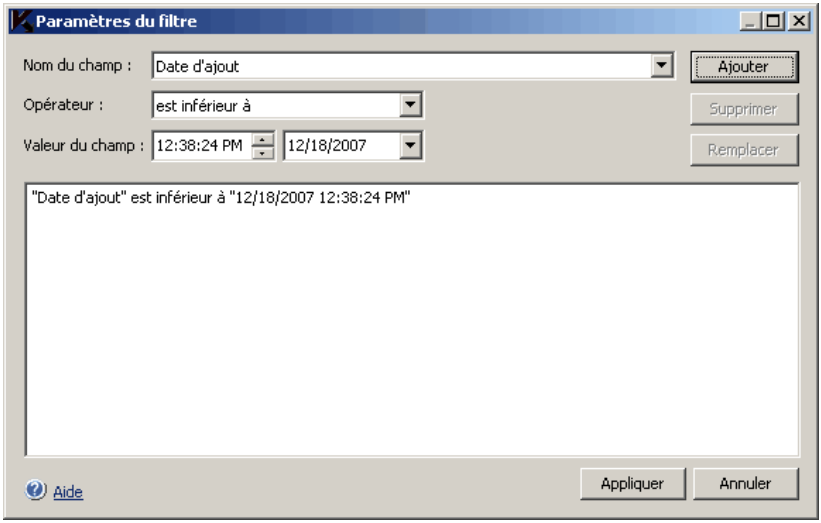

Illustration 65. Boîte de dialogue **Paramètres du filtre**

2. Pour ajouter un filtre :

   a) Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b) Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c) Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

   d) Cliquez sur **Ajouter**.

      Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Si vous définissez plusieurs filtres, ils seront unis par le lien logique « **ET** ».

- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**.

*Pour afficher à nouveau tous les objets dans la liste des objets en quarantaine, ouvrez le menu contextuel du noeud **Quarantaine** dans l'arborescence de la console puis, sélectionnez **Ôter le filtre**.*

11.3. Analyse des objets en quarantaine. Paramètres de la tâche *Analyse des objets en quarantaine*

Par défaut, Kaspersky Anti-Virus exécute la tâche prédéfinie **Analyse des objets en quarantaine** après chaque mise à jour des bases. Les paramètres de la tâches sont repris au tableau 8. Vous ne pouvez pas les modifier.

Vous pouvez modifier la programmation de la tâche **Analyse des objets en quarantaine** ou la lancer manuellement.

Suite à l'analyse des objets en quarantaine après la mis à jour des bases, Kaspersky Anti-Virus peut décider que certains d'entre eux sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés par Kaspersky Anti-Virus, auquel cas il exécutera les actions définies dans les paramètres de la tâche d'analyse à la demande **Analyse des objets en quarantaine** : **réparer, supprimer si la réparation est impossible**.

Tableau 8. Paramètres de la tâche **Analyse des objets en quarantaine**

Paramètre de la tâche Analyse des objets en quarantaine	**Valeur**
Couverture de l'analyse	Répertoire de quarantaine
Paramètres de sécurité	Identiques pour toutes les couvertures de l'analyse ; les valeurs possibles sont reprises au tableau 9.

Tableau 9. Paramètres de sécurité de la tâche **Analyse des objets en quarantaine**

Paramètre de sécurité	Valeur
Objets à analyser (cf. point B.3.2, p. 400)	Analyser tous les objets
Analyser uniquement les nouveaux objets et les objets modifiés (cf. point B.3.3, p. 402)	Activée
Actions à exécuter sur les objets infectés (cf. point B.3.5, p. 404)	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. point B.3.6, p. 406)	Rapport uniquement
Exclusion des objets (cf. point B.3.8, p. 410)	Non
Exclusion des menaces (cf. point B.3.9, p. 411)	Non
Durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413)	Non défini
Taille maximale de l'objet à analyser (cf. point B.3.11, p. 413)	Non défini
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. point B.3.2, p. 400)	En cours
Analyse des secteurs d'amorçage (cf. point B.3.2 , p. 400)	Désactivée
Application de la technologie iChecker (cf. point B.3.12, p. 414)	Désactivé
Application de la technologie iSwift (cf. point B.3.13, p. 415)	Désactivé

Paramètre de sécurité	Valeur
Traiter les objets composés (cf. point B.3.4, p. 402)	• Archives* ; • Archives SFX* ; • Objets compactés* ; • Les objets OLE intégrés* * L'analyse **Uniquement des objets neufs et modifiés** est activée.

11.4. Restauration des objets de la quarantaine

Kaspersky Anti-Virus place les objets suspects sous une forme cryptée dans le répertoire de quarantaine afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer n'importe quel objet de la quarantaine. La restauration d'un objet peut s'imposer dans les situations suivantes :

- Après l'analyse de la quarantaine à l'aide des bases actualisées, l'état d'un objet est devenu **Fausse alerte** ou **Réparé** ;
- Vous estimez que l'objet ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Anti-Virus n'isole plus cet objet lors des analyses ultérieures, il faut l'exclure du traitement dans la tâche **Protection en temps réel des fichiers** et des tâches d'analyse à la demande. Pour ce faire, indiquez l'objet en guise de valeur du paramètre de sécurité **Exclusion des objets** (selon le nom des fichiers) (cf. point B.3.8, p. 410) ou **Exclusion des menaces** (cf. point B.3.9, p. 411) dans ces tâches.

Lors de la restauration d'un objet, vous pouvez sélectionner l'emplacement où l'objet restauré sera conservé : dans le répertoire d'origine (par défaut), dans un dossier spécial de restauration sur le serveur protégé ou dans un autre dossier indiqué sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou sur un autre ordinateur du réseau.

Le dossier *Restaurer dans le dossier* est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce répertoire est défini dans les paramètres de la quarantaine (cf. point 11.8, p. 186).

Attention !

La restauration d'objets de la quarantaine peut entraîner l'infection de l'ordinateur.

Remarque

Si l'objet placé en quarantaine fait partie d'un objet composé (une archive par exemple), Kaspersky Anti-Virus ne l'inclut pas à nouveau dans cet objet lors de la restauration mais l'enregistre séparément dans le répertoire indiqué.

Vous pouvez restaurer l'objet en conservant une copie dans le répertoire de quarantaine afin de pouvoir l'utiliser ultérieurement, par exemple afin de pouvoir analyser une nouvelle fois l'objet après la mise à jour des bases.

Vous pouvez restaurer un ou plusieurs objets.

Pour restaurer des objets mis en quarantaine :

1. Dans l'arborescence de la console, sélectionnez le noeud **Quarantaine**.
2. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Pour restaurer un objet, ouvrez le menu contextuel de l'objet que vous souhaitez restaurer et sélectionnez la commande **Restaurer** ;
   - Pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **<Ctrl>** ou **<Shift>** puis, ouvrez le menu contextuel d'un des objets sélectionnés avant de choisir l'option **Restaurer**.

   La boîte de dialogue **Restauration de l'objet** s'ouvre (cf. ill. 66).

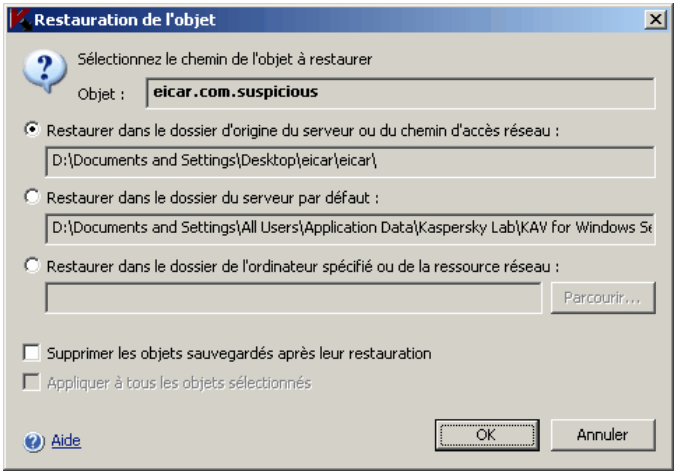

Illustration 66. Boîte de dialogue **Restauration de l'objet**

3. Dans la boîte de dialogue **Restauration de l'objet**, indiquez pour chaque objet sélectionné le répertoire dans lequel vous souhaitez conserver la copie restaurée (le nom de l'objet figure dans le champ **Objet** de la partie supérieure de la boîte de dialogue ; si vous avez sélectionné plusieurs objets, alors c'est le nom du premier objet de la liste qui est affiché).

   Exécutez une des actions suivantes :

   - Pour restaurer l'objet dans son emplacement d'origine, sélectionnez **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau** ;
   - Pour restaurer l'objet dans le répertoire que vous avez défini en tant que répertoire de restauration dans les paramètres de la quarantaine (cf. point B.6.4, p. 437), sélectionnez **Restaurer dans le dossier du serveur par défaut** ;
   - Pour enregistrer l'objet dans un autre répertoire de l'ordinateur où vous avez installé la console de Kaspersky Anti-Virus ou dans un répertoire de réseau, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** puis choisissez le répertoire souhaité ou saisissez le chemin d'accès à celui-ci.

4. Si vous souhaitez conserver une copie de l'objet dans le dossier de quarantaine après la restauration, désélectionnez la case **Supprimer les objets sauvegardés après leur restauration**.

5. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les objets sélectionnés seront restaurés et conservés dans l'emplacement que vous aurez défini : si vous avez choisi **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau** chacun des objets sera enregistré dans son répertoire d'origine ; si vous avez sélectionné **Restaurer dans le dossier du serveur par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, tous les objets seront conservés dans le dossier indiqué.

6. Cliquez sur **OK**.

   Kaspersky Anti-Virus commence par restaurer le premier des objets que vous avez sélectionnés.

7. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la boîte de dialogue **Un objet avec ce nom existe déjà** s'ouvre (cf. ill. 67).

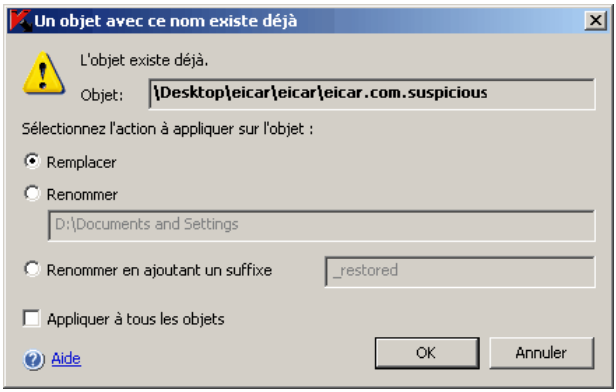

Illustration 67. Boîte de dialogue **Un objet avec ce nom existe déjà**

   a) Choisissez l'une des actions suivantes pour Kaspersky Anti-Virus :

      - **Remplacer** afin d'enregistrer l'objet restauré au lieu du fichier existant ;
      - **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet et son chemin d'accès dans le champ ;
      - **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

b) Si vous avez sélectionné plusieurs objets pour la restauration, alors pour appliquer l'action **Remplacer** ou **Renommer en ajoutant un suffixe** à tous les objets sélectionnés, cochez la case **Appliquer à tous les objets**. (Si vous avez sélectionné **Renommer**, alors la case **Appliquer à tous les objets** n'est pas accessible.)

c) Cliquez sur **OK**.

L'objet sera restauré ; les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets** dans la boîte de dialogue **Restauration de l'objet**, alors la boîte de dialogue **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 3 des présentes instructions).

11.5. Mise en quarantaine des fichiers

Vous pouvez mettre manuellement des fichiers en quarantaine.

Pour mettre des fichiers en quarantaine :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Quarantaine** et sélectionnez **Ajouter**.
2. Dans la boîte de dialogue **Ouvrir** sélectionnez les fichiers du disque que vous souhaitez placer en quarantaine puis, cliquez sur le bouton **OK**.

> **Remarque**
>
> Si les fichiers que vous voulez mettre en quarantaine se trouvent dans un même répertoire, alors la boîte de dialogue **Ouvrir** vous permet de sélectionner plusieurs fichiers à l'aide de la touche **<Ctrl>** ou **<Shift>**.

Kaspersky Anti-Virus placera le ou les fichier(s) sélectionné(s) en quarantaine.

3. Dans la boîte de dialogue portant le nom du premier fichier sélectionné, exécutez l'action suivante (si vous souhaitez appliquer l'action à tous les fichiers sélectionnés, cochez la case **Appliquer à tous les objets**) :

   - Pour enregistrer le fichier dans l'emplacement d'origine, cliquez sur le bouton **Enregistrer** ;

- Pour Supprimer le fichier de l'emplacement d'origine, cliquez sur le bouton **Supprimer**.

11.6. Suppression des objets de la quarantaine

Conformément aux paramètres de la tâche **Analyse des objets en quarantaine** (cf. point 11.3, p. 177), Kaspersky Anti-Virus supprime automatiquement du répertoire de quarantaine les objets dont l'état est devenu **Infecté** suite à l'analyse à l'aide des bases actualisées et qui n'ont pas pu être réparés. Kaspersky Anti-Virus ne supprime pas les autres objets.

Vous pouvez supprimer manuellement un ou plusieurs objets de la quarantaine.

Pour supprimer un ou plusieurs objets de la quarantaine :

1. Dans l'arborescence de la console, sélectionnez le noeud **Quarantaine**.
2. Exécutez une des actions suivantes :
   - Pour supprimer un objet, ouvrez le menu contextuel de l'objet que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;
   - Pour supprimer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **<Ctrl>** ou **<Shift>** puis, ouvrez le menu contextuel de n'importe lequel des objets sélectionnés avant de choisir l'option **Supprimer**.
3. Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

11.7. Envoi des objets suspects à Kaspersky Lab pour examen

Si le comportement d'un objet quelconque indique selon vous la présence éventuelle d'une menace et que Kaspersky Anti-Virus le considère comme un fichier sain, il se peut que vous soyez en présence d'un nouveau virus inconnu dont l'algorithme de réparation n'a pas encore été ajouté à la base. Vous pouvez envoyer ce fichier à Kaspersky Lab pour examen. Les experts antivirus de Kaspersky Lab analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de réparation aux bases. Il se peut que lors d'une analyse ultérieure après la mise à jour des bases que Kaspersky Anti-

Virus le considère comme un fichier infecté et parvienne à le réparer. Vous pourrez alors non seulement conserver l'objet mais également éviter une épidémie virale.

Seuls les fichiers de la quarantaine peuvent être envoyés pour examen. Ils sont conservés sous forme cryptée et pendant le transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

Vous pouvez envoyer pour examen les fichiers de la quarantaine auxquels Kaspersky Anti-Virus a attribué l'état Suspect ou Avertissement. Vous ne pouvez envoyer pour examen les fichiers de la quarantaine auxquels Kaspersky Anti-Virus a attribué l'état Infecté. Pour en savoir plus sur la façon dont Kaspersky Anti-Virus identifie les menaces dans les objets, lisez le point 1.1.3 à la page 20.

Remarque

Vous ne pouvez pas envoyer un objet de la quarantaine à Kaspersky Lab une fois que la clé de licence n'est plus valide.

Pour envoyer un fichier à Kaspersky Lab en vue d'un examen :

1. Si l'objet ne se trouve pas encore en quarantaine, il conviendra de l'y placer (cf. point 11.5, p. 183).
2. Dans le noeud **Quarantaine**, liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous voulez envoyer à Kaspersky Lab pour examen et sélectionnez l'option **Envoyer à Kaspersky Lab**.
3. Si un client de messagerie est configuré sur le poste où la console de Kaspersky Anti-Virus est installée, un nouveau message électronique sera créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

   Le champ **Destinataire** du message contient l'adresse électronique de Kaspersky Lab newvirus@kaspersky.com. Le champ **Objet** contient le texte « Objet de la quarantaine ». Le corps du message contient le texte « Le fichier sera envoyé à Kaspersky Lab pour examen ».

   Le corps du message contient le texte « Le fichier sera envoyé à Kaspersky Lab pour examen ». Vous pouvez ajouter au corps du message n'importe quelle information sur le fichier : pourquoi l'avez-vous trouvé suspect, comment se comporte-t-il ou quelle est son influence sur le système.

   Le message est accompagné de l'archive *<nom de l'objet>.cab*. Il contient le fichier *<uuid>.klq* avec l'objet crypté, le fichier *<uuid>.txt* avec les informations récoltées par Kaspersky Anti-Virus sur l'objet et le fichier *Sysinfo.txt* qui contient les informations relatives à Kaspersky Anti-Virus et au système d'exploitation du serveur :

   - Nom et version du système d'exploitation ;

- Nom et version de Kaspersky Anti-Virus ;
- Date d'édition des mises à jour des bases installées ;
- Numéro de série de la clé active.

Ces informations sont indispensables aux experts de Kaspersky Lab afin de pouvoir analyser le fichier le plus vite et le plus efficacement possible. Toutefois, si vous ne souhaitez pas les transmettre, vous pouvez supprimer le fichier *Sysinfo.txt* de l'archive.

4. Si le client de messagerie n'est pas configuré sur l'ordinateur où est installée la console de Kaspersky Anti-Virus, l'Assistant de connexion à Internet de Microsoft Windows s'ouvre. Vous pouvez exécuter les opérations suivantes :

   - Suivre les instructions de l'Assistant de connexion à Internet, créer un nouveau compte utilisateur et envoyer le fichier de cet ordinateur.
   - Quitter l'Assistant et enregistrer l'objet sélectionné crypté dans un fichier. Ce fichier peut être envoyé seul à Kaspersky Lab.

   Pour enregistrer l'objet crypté dans un fichier :

   a) Dans la boîte de dialogue qui vous invite à enregistrer l'objet (cf. ill. 68), cliquez sur le bouton **OK** ;

   b) Sélectionnez le répertoire sur le disque du serveur protégé ou le répertoire de réseau dans lequel vous souhaitez enregistrer le fichier avec l'objet.

Illustration 68. Boîte de dialogue avec invitation pour enregistrer l'objet en quarantaine dans un fichier

11.8. Configuration de la quarantaine

Cette section décrit la configuration des paramètres de la quarantaine. Les nouvelles valeurs des paramètres de la quarantaine sont appliquées directement après l'enregistrement.

La description des paramètres de la quarantaine et de leur valeur par défaut est reprise au point B.6, p. 434.

Pour configurer les paramètres de la quarantaine :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Quarantaine** et sélectionnez **Propriétés** (cf. ill. 69).

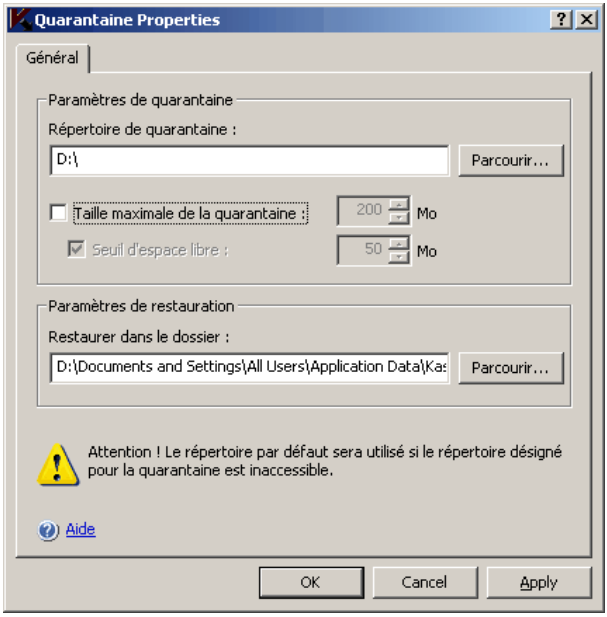

Illustration 69. Boîte de dialogue **Propriétés: Quarantaine**

2. Dans la boîte de dialogue **Propriétés: Quarantaine**, configurez les différents paramètres en fonction de vos besoins :

   - Pour définir un répertoire de quarantaine différent du répertoire proposé par défaut, sélectionnez le répertoire voulu sur le disque local du serveur protégé dans le champ **Répertoire de quarantaine** puis indiquez son nom et son chemin d'accès complet (pour de plus amples informations sur ce paramètre, lisez le point B.6.1 à la page 435) ;

   - Pour limiter la taille maximale de la quarantaine, cochez la case **Taille maximale de la quarantaine** et saisissez la valeur souhaitée en mégaoctets (cf. point B.6.2, p. 436) ;

   - Pour définir l'espace disponible minimum dans la quarantaine, déterminez le paramètre **Taille maximale de la quarantaine**, cochez

la case **Seuil d'espace libre** et saisissez la valeur souhaitée en mégaoctets dans le champ (cf. point B.6.3, p. 436) ;

- Pour désigner un autre répertoire de restauration, sélectionnez, dans le groupe de paramètres **Paramètres de restauration**, le répertoire souhaité sur le disque local du serveur protégé ou saisissez son nom et son chemin d'accès complet (cf. point B.6.4, p. 437).

3. Cliquez sur **OK**.

11.9. Statistiques de quarantaine

Vous pouvez consulter les informations relatives au nombre d'objets en quarantaine ; il s'agit des *statistiques de la quarantaine*.

*Pour consulter les statistiques de la quarantaine, ouvrez le menu contextuel du noeud **Quarantaine** dans l'arborescence de la console et sélectionnez **Voir les statistiques** (cf. ill. 70).*

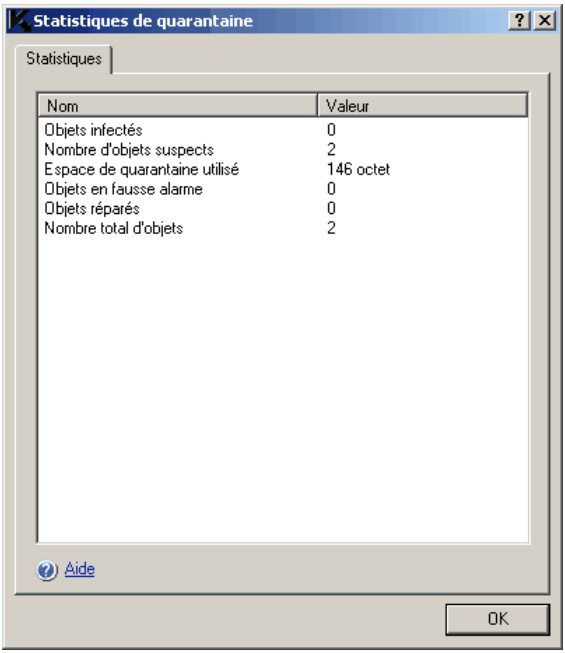

Illustration 70. Boîte de dialogue **Statistiques de quarantaine**

La boîte de dialogue **Statistiques de quarantaine** reprend les informations suivantes sur le nombre d'objets en quarantaine à l'heure actuelle.

Champ	Description
Objets infectés	Nombre d'objets infectés: a) qui ont reçu l'état *Infecté* après l'analyse de la quarantaine et que Kaspersky Anti-Virus n'a pas pu réparer ou supprimer et b) que Kaspersky Anti-Virus a placé en quarantaine conformément à la valeur du paramètre **Actions sur les objets en fonction du type de menace**.
Nombre d'objets suspects	Nombre d'objets suspects et présentant un risque potentiel. Pour en savoir plus sur la façon dont Kaspersky Anti-Virus identifie les menaces dans les objets, lisez le point 1.1.3 à la page 20.
Espace de quarantaine utilisé	Volume général de données dans le dossier de quarantaine
Objets en fausse alarme	Nombre d'objets qui ont reçu l'état **Fausse alerte** car l'analyse de la quarantaine à l'aide des bases actualisées a indiqué ces objets comme étant sains.
Objets réparés	Nombre d'objets qui ont reçu l'état **Réparé** après l'analyse de la quarantaine
Nombre total d'objets	Nombre total d'objets en quarantaine

CHAPITRE 12. SAUVEGARDE DES OBJETS AVANT LA REPARATION / LA SUPPRESSION. UTILISATION DE LA SAUVEGARDE

Le présent chapitre aborde les sujets suivants :

- Présentation de la sauvegarde des fichiers avant la réparation ou la suppression (cf. 12.1, p. 190) ;
- Consultation des fichiers en sauvegarde, tri et filtrage des fichiers (cf. point 12.2, p. 191) ;
- Restauration des fichiers de la sauvegarde (cf. point 12.3, p. 196) ;
- Suppression des fichiers de la sauvegarde (cf. point 12.4, p. 200) ;
- Configuration des paramètres de la sauvegarde (cf. point 12.5, p. 200) ;
- Statistiques de la sauvegarde (cf. point 12.6, p. 202) ;

Les paramètres de la sauvegarde sont présentés au point B.7 à la page 438.

12.1. Présentation de la sauvegarde des objets avant la réparation / la suppression

Avant de réparer ou de supprimer un fichier dont l'état est **Infecté**, Kaspersky Anti-Virus enregistre une copie cryptée de celui-ci dans un répertoire spécial : le *dossier de sauvegarde*.

Kaspersky Anti-Virus enregistre également dans le dossier de sauvegarde et sous forme cryptée une copie des fichiers dont l'état est **Suspect** ou **Potentiel-**

lement dangereux si dans les paramètres de sécurité de la tâche **Protection en temps réel des fichiers** ou des tâches d'analyse à la demande, vous avez sélectionné **Supprimer** en guise d'action à exécuter sur les objets suspects.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Anti-Virus enregistre cet objet composé dans la sauvegarde.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur le serveur protégé ou sur un autre ordinateur du réseau local. Vous pouvez restaurer le fichier du dossier de sauvegarde si, par exemple, le fichier original infecté contenait des informations cruciales et que lors de la réparation, Kaspersky Anti-Virus n'a pas réussi à le préserver, ce qui a rendu inaccessibles les informations qu'il contenait.

Attention !

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

12.2. Consultation des fichiers du dossier de sauvegarde

Vous pouvez consulter les fichiers du dossier de sauvegarde uniquement via la console de Kaspersky Anti-Virus dans le noeud **Sauvegarde**. Vous ne pouvez pas les consulter à l'aide des gestionnaires de fichiers de Microsoft Windows.

*Pour consulter les fichiers de la sauvegarde, sélectionnez le noeud **Sauvegarde** (cf. ill. 71) dans l'arborescence de la console.*

Pour trouver l'objet requis dans la liste, vous pouvez les trier (cf. point 12.2.1, p. 194) ou les filtrer (12.2.2, p. 194).

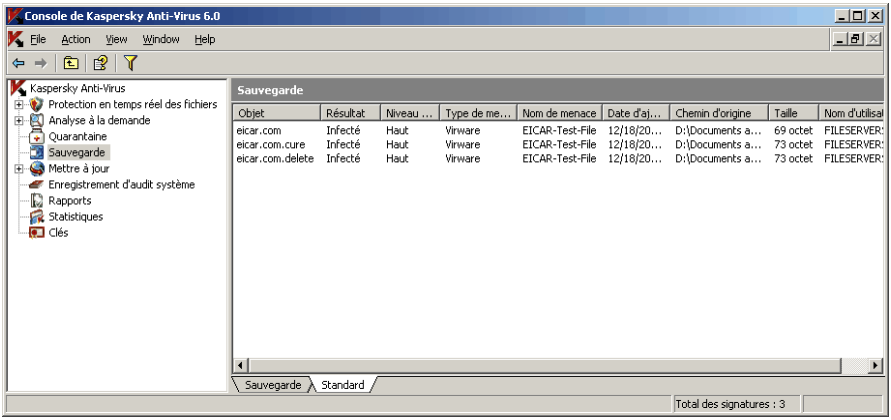

Illustration 71. Informations relatives aux fichiers dans la sauvegarde dans la console de Kaspersky Anti-Virus

Le panneau des résultats affiche les informations suivantes relatives aux fichiers de la sauvegarde :

Champ	Description
Objet	Nom du fichier dont une copie se trouve dans la sauvegarde
Résultat	Etat du fichier en ce qui concerne la présence ou nom de menaces : • **Infecté**. Le fichier est infecté ; il existe une équivalence parfaite entre une partie du code du fichier et une partie du code d'une menace connue. • **Suspect**. Le fichier est suspect; il existe une équivalence partielle entre une partie du code du fichier et une partie du code d'une menace connue. • **Potentiellement dangereux**. Le fichier est identifié comme potentiellement dangereux par l'analyseur heuristique de Kaspersky Anti-Virus. Pour en savoir plus sur la façon dont Kaspersky Anti-Virus identifie les menaces dans les objets, lisez le point 1.1.3 à la page 20.

Champ	Description
Niveau de danger	Le niveau de danger indique la menace que représente l'objet pour le serveur. Le niveau de danger dépend du type de menace dans l'objet et il peut avoir l'une des valeurs suivantes : • **Haut**. Le fichier contient une menace de type *vers de réseau*, *virus traditionnels*, *chevaux de Troie* ou une menace d'un type indéfini (par exemple, les nouveaux virus qui n'ont pour l'instant aucun lien avec les catégories connues) ; • **Moyen**. Le fichier peut contenir une menace du type *autres programmes malveillants*, *logiciels publicitaires* ou *programmes au contenu pornographique* ; • **Bas**. Le fichier peut contenir une menace du type *programmes présentant un risque potentiel*. Pour obtenir de plus amples informations sur les menaces découvertes par Kaspersky Anti-Virus, lisez le point 1.1.2 à la page 16.
Type de menace	Type de menaces selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un fichier comme étant infecté ou suspect. Vous pouvez obtenir le nom complet de la menace dans l'objet dans le rapport détaillé de l'exécution de la tâche. (noeud **Rapports**).
Nom de menace	Nom de la menace selon la classification de Kaspersky Lab ; figure dans le nom complet de la menace donné par Kaspersky Anti-Virus lorsqu'il a identifié un fichier comme étant infecté. Vous pouvez obtenir le nom complet de la menace dans l'objet dans le rapport détaillé de l'exécution de la tâche. (noeud **Rapports**).
Date de placement	Date et heure de l'enregistrement du fichier dans la sauvegarde
Chemin d'origine	Chemin d'accès complet au répertoire d'origine : répertoire où se trouvait le fichier avant que sa copie ne soit placée par Kaspersky Anti-Virus dans la sauvegarde
Taille	Taille du fichier

Champ	Description
Nom d'utilisateur	Cette colonne reprend les données suivantes : • Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche **Protection en temps réel des fichiers** – nom du compte utilisateur sous les privilèges duquel l'application a sollicité le fichier au moment de l'interception ; • Si Kaspersky Anti-Virus a mis l'objet en sauvegarde dans la tâche d'analyse à la demande – nom du compte utilisateur sous les privilèges duquel la tâche a été exécutée.

Pour en savoir plus sur la configuration des paramètres de la sauvegarde, consultez le point 12.5 à la page 200.

12.2.1. Tri des fichiers de la sauvegarde

Par défaut, les fichiers de la sauvegarde sont classés par date d'enregistrement dans l'ordre chronologique inversé. Pour trouver le fichier requis, vous pouvez trier les fichiers selon le contenu de n'importe quelle colonne dans le panneau des résultats.

Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Sauvegarde**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour trier les fichiers dans la sauvegarde :

1. Dans l'arborescence de la console, sélectionnez le noeud **Sauvegarde**.
2. Dans la liste des fichiers de la sauvegarde, cliquez sur le titre de la colonne selon laquelle vous souhaitez trier les objets.

12.2.2. Filtrage des fichiers de la sauvegarde

Pour trouver le fichier qu'il vous faut dans la sauvegarde, vous pouvez *filtrer* les fichiers, c.-à-d. afficher dans le noeud **Sauvegarde** uniquement les fichiers qui répondent aux conditions de filtrage que vous avez définies (les filtres).

Les résultats du filtrage sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Sauvegarde**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour filtrer les fichiers dans la sauvegarde :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Sauvegarde** et sélectionnez **Filtre**.

   La boîte de dialogue **Paramètres du filtre** s'ouvre (cf. ill. 72).

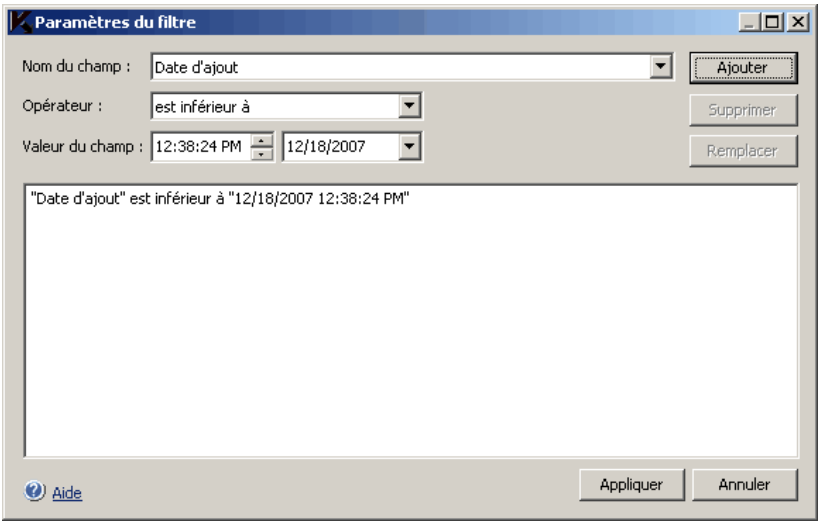

Illustration 72. Boîte de dialogue **Paramètres du filtre**

2. Pour ajouter un filtre, exécutez les opérations suivantes :

   a) Dans la liste **Nom du champ**, sélectionnez le champ dont la valeur sera comparée à la valeur du filtre.

   b) Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans le champ **Nom du champ**.

   c) Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la.

   d) Cliquez sur **Ajouter**.

      Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre

que vous souhaitez ajouter. Si vous définissez plusieurs filtres, ils seront unis par le lien logique « ET ».

- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les fichiers qui répondent aux conditions des filtres.

*Pour afficher à nouveau tous les fichiers dans la liste des fichiers de la sauvegarde, ouvrez le menu contextuel du noeud **Sauvegarde** dans l'arborescence de la console puis, sélectionnez **Ôter le filtre**.*

12.3. Restauration des fichiers depuis la sauvegarde

Kaspersky Anti-Virus place les fichiers sous une forme cryptée dans la sauvegarde afin de protéger le serveur contre une éventuelle action malveillante.

Vous pouvez restaurer les fichiers de la sauvegarde.

La restauration d'un fichier peut s'imposer dans les situations suivantes :

- Si le fichier original, qui était infecté, contenait des informations importantes et que Kaspersky Anti-Virus n'a pas pu préserver son intégrité lors de la réparation, ce qui a rendu les informations du fichier inaccessibles ;
- Vous estimez que le fichier ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Anti-Virus ne considère plus ce fichier comme un fichier infecté ou suspect lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche **Protection en temps réel des fichiers** et dans les tâches d'analyse à la demande. Pour ce faire, indiquez le fichier en guise de valeur du paramètre **Exclusion des objets** (cf. point B.3.8, p. 410) ou **Exclusion des menaces** (cf. point B.3.9, p. 411).

Attention !

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où il sera conservé : dans le répertoire d'origine (par défaut), dans un dossier spécial pour la restauration des objets sur le serveur protégé ou dans un autre dossier indiqué sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou sur un autre ordinateur du réseau.

Le dossier *Restaurer dans le dossier* est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce dossier est défini par les paramètres de la sauvegarde (pour savoir comment les configurer, consultez le point 12.5 à la page 200).

Par défaut, lorsque Kaspersky Anti-Virus restaure le fichier, il supprime sa copie de la sauvegarde. Vous pouvez conserver la copie du fichier dans la sauvegarde après sa restauration.

Pour restaurer des fichiers depuis la sauvegarde :

1. Dans l'arborescence de la console, sélectionnez le noeud **Sauvegarde**.
2. Exécutez une des actions suivantes :
   - Pour restaurer un fichier, ouvrez le menu contextuel du fichier, dans la liste des fichiers de la sauvegarde, que vous souhaitez restaurer et sélectionnez la commande **Restaurer** ;
   - Pour restaurer plusieurs fichiers, sélectionnez les fichiers souhaités dans la liste à l'aide de la touche **<Ctrl>** ou **<Shift>** puis, ouvrez le menu contextuel d'un des fichiers sélectionnés avant de choisir l'option **Restaurer**.
3. Dans la boîte de dialogue **Restauration de l'objet** (cf. ill. 73), précisez le répertoire dans lequel le fichier restauré sera enregistré.

   Le nom du fichier apparaît dans le champ **Objet** de la partie supérieure de la boîte de dialogue. Si vous avez sélectionné plusieurs fichiers, alors c'est le nom du premier fichier de la sélection qui apparaîtra.

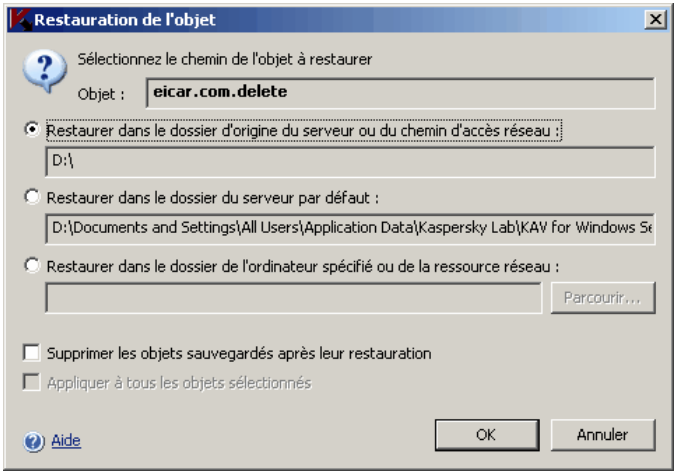

Illustration 73. Boîte de dialogue **Restauration de l'objet**

Exécutez une des actions suivantes :

- Pour enregistrer le fichier restauré sur le serveur protégé, sélectionnez :
  - **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau,** si vous souhaitez restaurer le fichier dans son répertoire d'origine ;
  - **Restaurer dans le dossier du serveur par défaut** si vous souhaitez restaurer le fichier dans le répertoire que vous avez désigné en tant que répertoire de restauration dans les paramètres de la sauvegarde (cf. point 12.5, p. 200).
- Pour enregistrer le fichier restauré dans un autre répertoire, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau** puis choisissez le répertoire souhaité (sur l'ordinateur où est installée la console de Kaspersky Anti-Virus ou dans un répertoire de réseau) ou saisissez le chemin d'accès à celui-ci.

4. Si vous souhaitez conserver une copie du fichier dans la sauvegarde après la restauration, désélectionnez la case **Supprimer les objets sauvegardés après leur restauration**.
5. Si vous avez sélectionné plusieurs fichiers pour la restauration, alors pour appliquer les conditions de conservation définies aux autres fichiers sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

Tous les fichiers sélectionnés seront restaurés et conservés dans le répertoire que vous aurez défini : si vous avez choisi **Restaurer dans le dossier d'origine du serveur ou du chemin d'accès réseau**, chacun des fichiers sera enregistré dans son répertoire d'origine ; si vous avez sélectionné **Restaurer dans le dossier du serveur par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, tous les fichiers seront conservés dans le dossier indiqué.

6. Cliquez sur **OK**.

   Kaspersky Anti-Virus commence par restaurer le premier des fichiers que vous avez sélectionné.

7. Si un fichier portant le même nom existe déjà dans le répertoire indiqué, la boîte de dialogue **Un objet avec ce nom existe déjà** s'ouvre (cf. ill. 74).

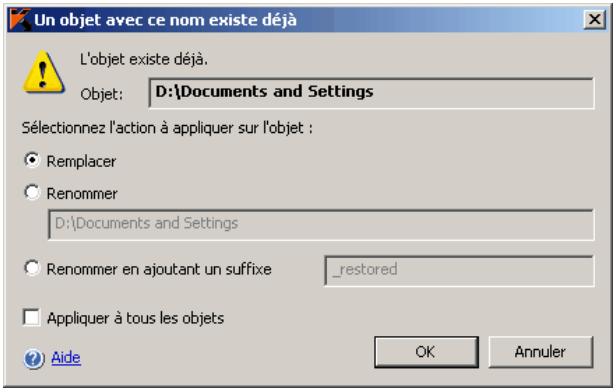

Illustration 74. Boîte de dialogue **Un objet avec ce nom existe déjà**

Exécutez les actions suivantes :

a) Sélectionnez les conditions d'enregistrement du fichier restauré :

   - **Remplacer** afin d'enregistrer le fichier restauré au lieu du fichier existant ;
   - **Renommer** afin d'enregistrer le fichier restauré sous un autre nom. Saisissez le nouveau nom du fichier et son chemin d'accès complet dans le champ ;
   - **Renommer en ajoutant un suffixe** afin de renommer le fichier en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

b) Si vous souhaitez appliquer l'action **Remplacer** au **Renommer en ajoutant un suffixe** aux fichiers restants, cochez la case **Appli-**

quer à tous les objets (si vous avez sélectionné **Renommer**, alors la case **Appliquer à tous les objets** n'est pas accessible)

c) Cliquez sur **OK**.

Le fichier sera restauré. Les informations relatives à la restauration seront consignées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets** dans la boîte de dialogue **Restauration de l'objet**, alors la boîte de dialogue **Restauration de l'objet** s'ouvrira à nouveau. Vous pourrez y indiquer le répertoire dans lequel le prochain fichier de la sélection sera enregistré après la restauration (cf. étape 3 des présentes instructions).

12.4. Suppression des fichiers depuis la sauvegarde

Pour supprimer un ou plusieurs fichiers de la sauvegarde :

1. Dans l'arborescence de la console, sélectionnez le noeud **Sauvegarde**.
2. Exécutez une des actions suivantes :
   - Pour supprimer un fichier, ouvrez le menu contextuel du fichier que vous souhaitez supprimer dans la liste des objets et sélectionnez la commande **Supprimer** ;
   - Pour restaurer plusieurs fichiers, sélectionnez les fichiers souhaités dans la liste à l'aide de la touche **<Ctrl>** ou **<Shift>** puis, ouvrez le menu contextuel de n'importe lequel des fichiers sélectionnés avant de choisir l'option **Supprimer**.
3. Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération. Les fichiers sélectionnés seront supprimés.

12.5. Configuration des paramètres de la sauvegarde

Cette section décrit la marche à suivre pour configurer les paramètres de la sauvegarde. La description des paramètres de la sauvegarde et de leur valeur par défaut est reprise au point B.7, p. 438.

Les nouvelles valeurs des paramètres de la sauvegarde sont appliquées directement après l'enregistrement.

Pour configurer les paramètres de la sauvegarde :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Sauvegarde** et sélectionnez **Propriétés** (cf. ill. 75).

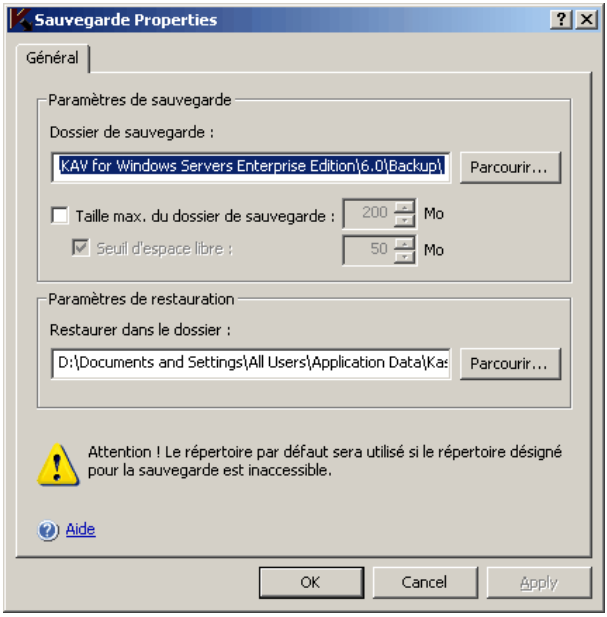

Illustration 75. Boîte de dialogue **Propriétés: Sauvegarde**

2. Dans la boîte de dialogue **Propriétés : Sauvegarde**, exécutez les opérations suivantes :

   - Pour définir le répertoire qui accueillera la sauvegarde, cliquez dans le champ **Dossier de sauvegarde** et indiquez le répertoire voulu sur le disque local du serveur protégé ou saisissez le chemin d'accès complet à celui-ci (pour de plus amples informations sur le paramètre, lisez le point B.7.1 à la page 438) ;

   - Pour modifier la taille maximale de la sauvegarde, cochez la case **Taille max. du dossier de sauvegarde** et saisissez la valeur souhaitée en mégaoctets (cf. point B.7.2, p. 439) ;

   - Pour définir le seuil d'espace disponible dans la sauvegarde, cochez la case **Taille max. du dossier de sauvegarde**, cochez la case **Seuil d'espace libre** et saisissez la valeur minimale souhai-

tée disponible dans la sauvegarde en mégaoctets (cf. point B.7.3, p. 440) ;

- Pour indiquer le répertoire de restauration des objets, dans le groupe de paramètres **Paramètres de restauration**, sélectionnez le répertoire requis sur le disque local du serveur protégé ou dans le champ **Restaurer dans le dossier**, saisissez le nom du dossier et son chemin d'accès complet (cf. point B.7.4, p. 441).

3. Cliquez sur **OK**.

12.6. Statistiques de sauvegarde

Vous pouvez consulter les informations relatives à l'état de la sauvegarde en ce moment ; il s'agit des *statistiques de la sauvegarde*.

Pour consulter les statistiques de la sauvegarde, dans l'arborescence de la console, ouvrez le menu contextuel du noeud ***Sauvegarde*** *et sélectionnez* ***Voir les statistiques*** *(cf. ill. 76).*

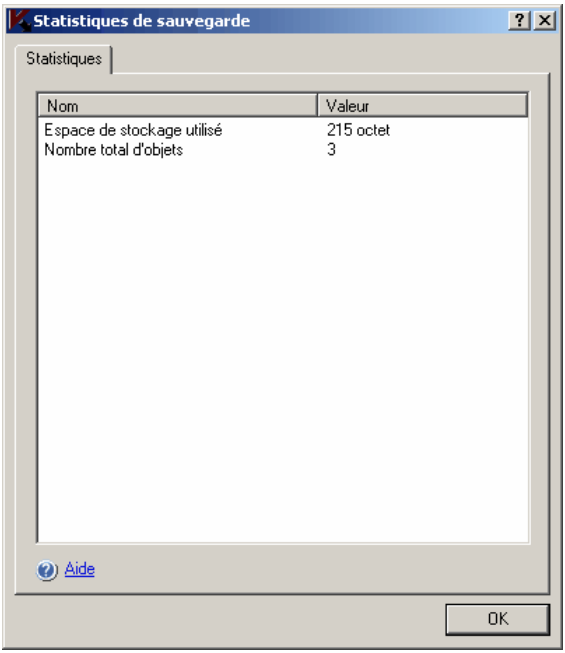

Illustration 76. Boîte de dialogue **Statistiques de sauvegarde**

Dans la boîte de dialogue **Statistiques de sauvegarde**, vous pourrez voir les informations suivantes relatives à l'état de la sauvegarde à ce moment :

Tableau 10. Statistiques de sauvegarde

Champ	Description
Espace de stockage utilisé	Volume de données présentes dans la sauvegarde
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde

CHAPITRE 13. CONSIGNATION DES EVENEMENTS

Le présent chapitre aborde les sujets suivants :

- Présentation des moyens d'enregistrement des événements dans Kaspersky Anti-Virus (cf. point 13.1, p. 204) ;
- Rapports sur l'exécution des tâches : consultation, suppression et configuration (cf. point 13.2, p. 205) ;
- Journal d'audit système : consultation, purge (cf. point 13.3, p. 219) ;
- Statistiques de Kaspersky Anti-Virus : informations sur l'état actuel de Kaspersky Anti-Virus, ses composants et les tâches exécutées (cf. point 13.4, p. 224) ;
- Journal des événements de Kaspersky Anti-Virus dans la console MMC « Consultation des événements » Microsoft Windows (cf. point 13.5, p. 228).

13.1. Moyens d'enregistrement des événements

Les événements dans Kaspersky Anti-Virus sont scindés entre les événements liés au traitement des objets dans les tâches et les événements liés à l'administration de Kaspersky Anti-Virus. Il s'agit également des événements tels que le lancement de Kaspersky Anti-Virus, la création ou la suppression de tâches, l'exécution de tâche, la modification des paramètres des tâches, etc.

Kaspersky Anti-Virus consigne les événements de la manière suivante :

- Il crée des *rapports sur l'exécution des tâches*. Un rapport sur l'exécution d'une tâche contient des informations sur l'état actuel de la tâche et sur les événements survenus durant l'exécution (cf. point 13.2, p. 205) ;
- Tient un *journal d'audit système* ; ce journal reprend les événements liés à l'administration de Kaspersky Anti-Virus (cf. point 13.3, p. 219) ;
- Récolte les *statistiques* relatives à son fonctionnement ; il s'agit des informations sur l'état actuel des composants fonctionnels et sur l'état des tâches en cours d'exécution à ce moment (cf. point 13.4, p. 224) ;

- Tient un j*ournal des événements* dans la console « Event Viewer » de Microsoft Windows dans lequel il consigne les événements importants pour le diagnostic des échecs (cf. point 13.5, p. 228).

Si un problème survient durant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus ou une tâche particulière s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un *fichier de traçage* et un *fichier de vidage de la mémoire des processus de Kaspersky Anti-Virus* et envoyer ces fichiers avec ces informations au service d'assistance technique de Kaspersky Lab pour analyse. Pour en savoir plus sur la création d'un *fichier de traçage* et de *fichiers de vidage de mémoire*, lisez le Chapitre 3 à la page 45.

13.2. Rapports sur l'exécution des tâches

Cette section aborde les sujets suivants :

- Présentation des rapports sur l'exécution des tâches (cf. point 13.2.1, p. 205) ;
- Consultation des rapports de synthèse (cf. point 13.2.2, p. 206) ;
- Tri des rapports de synthèse dans la liste (cf. point 13.2.3, p. 209) ;
- Consultation des rapports détaillés dans les tâches (cf. point 13.2.4, p. 211) ;
- Exportation des informations du rapport détaillé dans un fichier texte (cf. point 13.2.5, p.216) ;
- Suppression des rapports (cf. point 13.2.5, p. 216) ;
- Modification du niveau de détail des informations des rapports sur l'exécution des tâches des composants individuels et du journal des événements (cf. point 13.2.7, p. 217).

13.2.1. Présentation des rapports sur l'exécution des tâches

Le noeud **Rapports** vous donne accès aux rapports de synthèse et aux rapports détaillés sur l'exécution des tâches de Kaspersky Anti-Virus. Un *rapport de synthèse* est une ligne d'informations sur l'état de la tâche et sur l'état global des objets traités du point de vue de la sécurité antivirus. *Le rapport détaillé* contient

les statistiques de l'exécution de la tâche (informations sur le nombre d'objets traités), les informations relatives à chaque objet traité par Kaspersky Anti-Virus depuis le lancement de la tâche jusqu'à maintenant ainsi que les paramètres de la tâche.

Par défaut, les rapports sont conservés durant une période déterminée. Dans les rapports détaillés relatifs aux tâches en cours d'exécution, les enregistrements relatifs aux événements survenus il y a plus de 30 jours sont supprimés. Les rapports de synthèse sur les tâches sont supprimés 30 jours après la fin des tâches. Grâce aux paramètres de Kaspersky Anti-Virus, vous pouvez modifier la durée de conservation des rapports ou désactiver la suppression automatique de ceux-ci afin de les conserver pour une durée indéterminée (cf. Chapitre 3, p. 45). Vous pouvez également sélectionner un rapport et le supprimer manuellement.

13.2.2. Consultation des rapports de synthèse. Etat des rapports de synthèse

Pour consulter le rapport de synthèse sur l'exécution de la tâche :

1. Dans l'arborescence de la console, sélectionnez le noeud **Rapports** (cf. ill. 77).

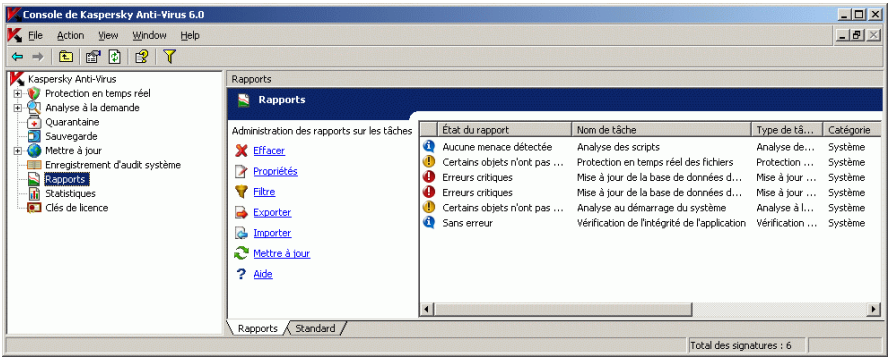

Illustration 77. Liste des rapports dans le panneau des résultats

2. Dans le panneau des résultats, identifiez le rapport requis sur la tâche (pour le trouver rapidement, vous pouvez filtrer les enregistrements ou les trier selon le contenu d'une des colonnes).

   Pour en savoir plus sur la consultation du rapport détaillé de l'exécution d'une tâche, consultez le point 13.2.4 à la page 211.

Le rapport contient les informations suivantes sur l'exécution de la tâche :

Tableau 11. Information sur l'exécution de la tâche dans le rapport

Champ	Description
État du rapport	Brève caractéristique qui repose sur les statistiques de la tâche ; affiche l'état global des objets traités du point de vue de la sécurité antivirale. En fonction du niveau d'importance, les rapports sont classés dans les catégories suivantes : *information*, *avertissement* ou *critique*. Les tableaux suivants décrivent les états du rapport sur les tâches d'analyse à la demande et sur les tâches de mise à jour.
Nom de tâche	Nom de la tâche dont vous souhaitez consulter le rapport.
Type de tâche	Le type de tâche correspond au composant fonctionnel dans lequel la tâche est créée (protection en temps réel des fichiers, analyse des scripts, analyse à la demande, mise à jour).
Catégorie de tâche	Catégorie de tâche dans Kaspersky Anti-Virus : *prédéfinie*, *définie par l'utilisateur* ou *de groupe*. Pour obtenir de plus amples informations sur les types de tâches, lisez le point 5.1 à la page 54.
État de la tâche	Etat de la tâche à ce moment : *En exécution, Terminée, Pause, Arrêtée, Terminée sur un échec, Lancée, Relancée.*
Heure de fin	Si la tâche est terminée, alors cette colonne reprend la date et l'heure de fin. Si à ce moment, la tâche est exécutée, alors le champ est vide.

Tableau 12. États des rapports sur les tâches d'analyse à la demande

Degré d'importance	État du rapport	Description de l'état du rapport
	Aucune menace n'a été découverte	Kaspersky Anti-Virus a analysé tous les objets du secteur sélectionné. Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains.

Degré d'importance	État du rapport	Description de l'état du rapport
	Certains objets n'ont pas été traités	Kaspersky Anti-Virus considère tous les objets analysés comme sains ; un ou plusieurs objets ont été ignorés, par exemple parce qu'ils étaient exclus de l'analyse par les paramètres de sécurité ou parce qu'ils étaient utilisés par d'autres applications au moment de l'analyse. Lors de la requête, les fichiers système Windows peuvent être utilisés. Kaspersky Anti-Virus ne les analyse pas et la tâche se termine sur l'état *Certains objets n'ont pas été traités*.
	Objets endommagés détectés	Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains. Un ou plusieurs objets du secteur sélectionné ont été ignorés : Kaspersky Anti-Virus n'a pas réussi à lire ces objets car leur format est corrompu.
	Objets suspects détectés	Kaspersky Anti-Virus considère un ou plusieurs objets analysés comme étant suspects. Vous pouvez voir quels sont les objets suspects en consultant le rapport sur l'exécution de la tâche (cf. point 13.2.4, p. 211).
	Objets infectés détectés	Kaspersky a découvert des menaces dans un ou plusieurs objets. Vous pouvez voir quels sont les objets qui contiennent les menaces en consultant le rapport détaillé sur l'exécution de la tâche (cf. point 13.2.4, p. 211).

Degré d'importance	État du rapport	Description de l'état du rapport
	Erreurs de traitement	Kaspersky Anti-Virus a identifié tous les objets analysés comme étant sains. Pendant l'analyse d'un ou de plusieurs objets, une erreur est survenu dans Kaspersky Anti-Virus. **Remarque** L'objet analysé lorsque l'erreur s'est produit peut contenir une menace. Il est conseillé de placer cet objet en quarantaine et de l'analyser à nouveau après la mise à jour des bases (cf. point 11.3, p. 177). Si l'erreur se reproduit, contactez le service d'assistance technique de Kaspersky Lab. Pour obtenir de plus amples informations sur la manière de contacter le service d'assistance technique, consultez le point 1.2.3 à la page 24.
	Erreurs critiques	La tâche s'est soldée par un échec. Vous pouvez voir la cause de l'erreur dans le rapport détaillé sur l'exécution de la tâche.

Tableau 13. Etats des rapports des tâches de mise à jour des base et de copie des mises à jour

Degré d'importance	Etat du rapport	Description de l'état du rapport
	Sans erreur	Kaspersky Anti-Virus a récupéré et installé les mises à jour.
	Erreurs critiques	Une erreur s'est produite lors de la récupération ou de l'application des mises à jour. Le rapport détaillé sur l'exécution des tâches reprend le nom des mises à jour qui n'ont pas été appliquées et les causes de l'échec.

Tableau 14. Etat des rapports sur les tâches de mise à jour des modules de l'application

Degré d'importance	Etat du rapport	Description de l'état du rapport
	Sans erreur	Kaspersky Anti-Virus a récupéré et installé les mises à jour.
	Mise à jour critique disponible	Des mises à jour urgentes des modules de Kaspersky Anti-Virus ont été publiées.
	Une mise à jour prévue des modules d'application est disponible	Des mises à jour prévues des modules de Kaspersky Anti-Virus ont été publiées.
	Des mises à jour critiques et prévues sont disponibles	Des mises à jour urgentes et prévues des modules de Kaspersky Anti-Virus ont été publiées.
	L'installation des mises à jour récupérées est en cours	Kaspersky Anti-Virus a récupéré les mises à jour et les installe.
	La finalisation du processus de mise à jour requiert le redémarrage du serveur	Redémarrez le serveur pour appliquer les mises à jour.
	Erreurs critiques	Une erreur s'est produite lors de la récupération ou de l'application des mises à jour. Le rapport détaillé sur l'exécution des tâches reprend le nom des mises à jour qui n'ont pas été appliquées et les causes de l'échec.

13.2.3. Tri des rapports

Les rapports sont classés par défaut dans la liste dans l'ordre chronologique inverse. Vous pouvez classer les rapports selon le contenu de n'importe quelle colonne. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Rapports**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour trier les rapports :

1. Dans l'arborescence de la console, sélectionnez le noeud **Rapports**.

2. Dans le panneau d'informations, cliquez sur le titre de la colonne selon laquelle vous souhaitez trier les rapports de la liste.

13.2.4. Consultation du rapport détaillé sur l'exécution de la tâche

Le rapport détaillé sur l'exécution de la tâche reprend les informations relatives à tous les événements survenus dans la tâche depuis son lancement jusque maintenant. Par exemple, vous pouvez voir le nom des objets traités dans lesquels une menace a été découverte.

Pour consulter le rapport détaillé sur l'exécution de la tâche :

1. Dans l'arborescence de la console, sélectionnez le noeud **Rapports**.
2. Dans la liste des rapports, ouvrez le menu contextuel du rapport de synthèse des événements dont vous souhaitez consulter le rapport détaillé et sélectionnez l'option **Voir le rapport**.

La boîte de dialogue **Rapport détaillé** contient l'onglet **Evénements** qui reprend les informations sur les événements survenus pendant la tâche, l'onglet **Statistiques** qui reprend l'heure de début et de fin de la tâche et ses statistiques et l'onglet **Paramètres** avec les paramètres de la tâche.

L'onglet **Evénements** contient les informations suivantes sur les événements survenus pendant l'exécution de la tâche (cf. ill. 78) :

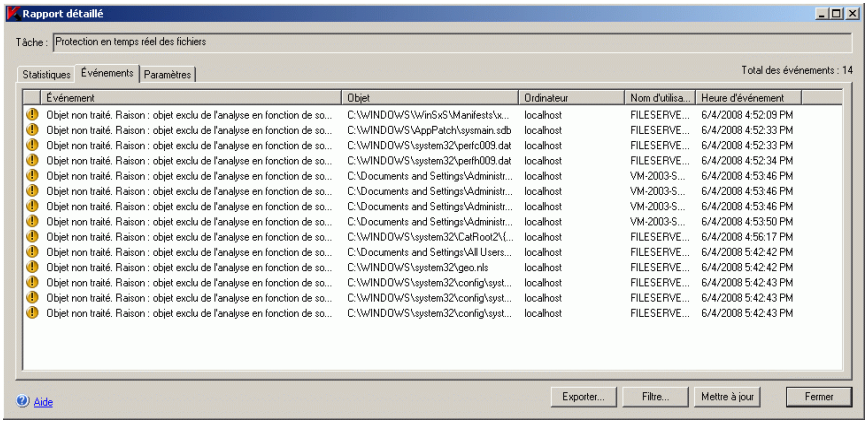

Illustration 78. Exemple de rapport détaillé de la tâche **Protection en temps réel des fichiers**

Le rapport détaillé sur les événements de la tâche contient les informations suivantes :

Champ	Description
Degré d'importance de l'événement	Les événements du rapport détaillés sont classés selon les catégories suivantes en fonction du degré d'importance : *informations*, *importants* ou *critiques*.
Objet	Nom de l'objet traité et chemin d'accès. Pour la tâche **Analyse des scripts**, cette colonne reprend également l'identificateur du processus (PID) qui a exécuté le script intercepté par Kaspersky Anti-Virus.
Événement	Type d'événement et informations complémentaires sur l'événement.
Heure d'événement	Date et heure auxquelles l'événement s'est produit.

Le rapport détaillé de la tâche **Protection en temps réel des fichiers** contient en plus des champs indiqués ci-dessus les champs **Ordinateur** et **Nom d'utilisateur** ; le rapport détaillé de la tâche **Analyse des scripts** contient le champ **Nom d'utilisateur** :

Champ	Description
Ordinateur	Nom de l'ordinateur d'où l'application a sollicité l'objet.
Nom d'utilisateur	Nom de l'utilisateur sous le compte duquel l'application a sollicité l'objet. Si l'objet a été sollicité par une application tournant sous le compte **Système local** (**SYSTEM**), alors cette colonne contiendra l'enregistrement <domaine><nom du poste>$. Dans la tâche **Protection en temps réel des fichiers**, Kaspersky Anti-Virus enregistre la valeur localhost en guise de nom de l'ordinateur et non pas le nom de réseau du serveur protégé si l'objet est sollicité par une application qui fonctionne sur le serveur protégé.

Pour consulter les statistiques de la tâche, ouvrez l'onglet ***Statistiques*** *(cf. ill. 79) dans la boîte de dialogue* ***Rapport détaillé****.*

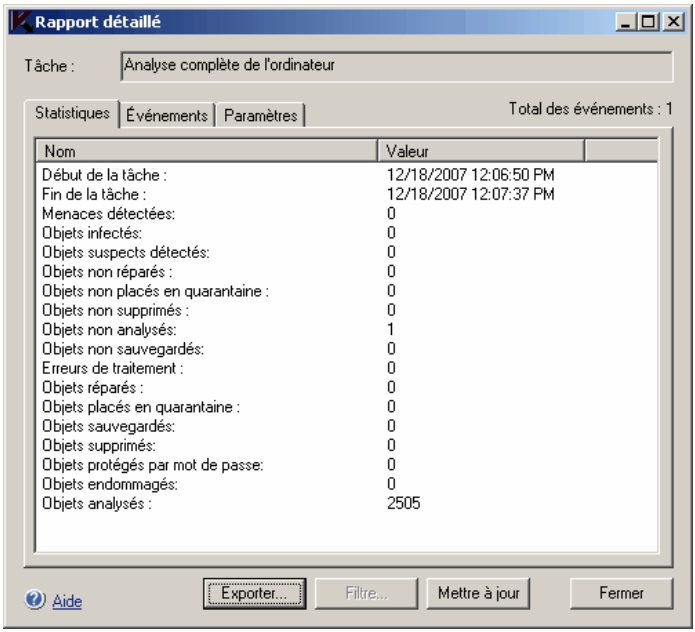

Illustration 79. Boîte de dialogue **Rapport détaillé**, onglet **Statistiques**

*Pour consulter les paramètres de la tâche, ouvrez l'onglet **Paramètres** (cf. ill. 80) dans la boîte de dialogue **Rapport détaillés**.*

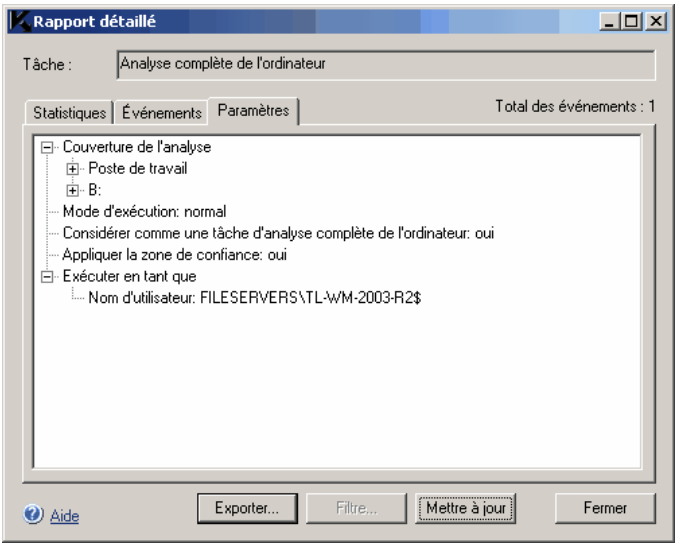

Illustration 80. Boîte de dialogue **Rapport détaillé**, onglet **Paramètres**

Lors de la consultation du rapport détaillé, vous pouvez définir un ou plusieurs filtres pour trouver l'événement souhaité dans l'onglet **Evénements**.

Pour définir un ou plusieurs filtres :

1. Cliquez sur le bouton **Filtre** dans la partie inférieure de la boîte de dialogue **Rapport détaillé**. La boîte de dialogue **Paramètres du filtre** s'ouvre (cf. ill. 81).

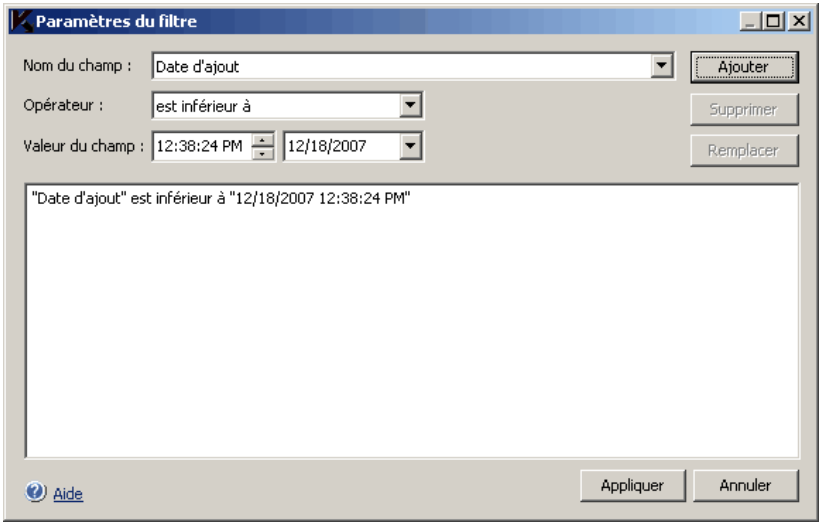

Illustration 81. Boîte de dialogue **Paramètres du filtre**

2. Pour ajouter un filtre :

   a) Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

   b) Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans le champ **Nom du champ**.

   c) Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste des valeurs disponibles.

   d) Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter.

- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Rechercher un objet**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste des objets du rapport détaillé reprendra uniquement les objets qui répondent aux conditions des filtres.

*Pour afficher à nouveau tous les objets, cliquez sur le bouton **Ôter le filtre** dans la partie inférieure de la boîte de dialogue **Rapport détaillé**.*

13.2.5. Exportation des informations du rapport détaillé dans un fichier texte

Pour exporter les infomrations du rapport détaillé dans un fichier texte :

1. Dans l'arborescence de la console, sélectionnez le noeud **Rapports**.
2. Dans la liste des rapports, ouvrez le menu contextuel du rapport de synthèse sur la tâche dont vous souhaitez consulter le rapport détaillé et cliquez sur **Voir le rapport**.
3. Dans la partie inférieure de la boîte de dialogue **Rapport détaillé** , cliquez sur le bouton **Exporter** et dans la boîte de dialogue **Parcourir,** saisissez le nom du fichier dans lequel vous souhaitez enregistrer les données du rapport détaillé et choisissez le code (Unicode ou ANSI).

13.2.6. Suppression des rapports

Par défaut, les rapports sont conservés durant une période définie (vous pouvez modifier celle-ci à l'aide du paramètre général de Kaspersky Anti-Virus **Durée de conservation des rapports**, cf. point 3.2, p. 46).

Le noeud **Rapports** vous permet de supprimer les rapports sélectionnés sur les tâches réalisées.

Pour supprimer un ou plusieurs rapports :

1. Dans l'arborescence de la console, sélectionnez le noeud **Rapports**.
2. Exécutez une des actions suivantes :
   - Pour supprimer un rapport, ouvrez le menu contextuel du rapport que vous souhaitez supprimer dans la liste des rapports et sélectionnez la commande **Supprimer** ;
   - Pour supprimer plusieurs rapports, sélectionnez les rapports souhaités à l'aide de la touche **<Ctrl>** ou **<Shift>** puis, ouvrez le menu contextuel de n'importe lequel des rapports sélectionnés avant de choisir l'option **Supprimer**.

Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération. Les rapports sélectionnés seront supprimés.

13.2.7. Configuration du niveau de détail des informations dans les rapports et le journal des événements

A l'aide des paramètres décrits ci-après, vous pouvez définir les événements qui seront consignés dans les rapports détaillés sur l'exécution des tâches des fonctions individuelles des composants de Kaspersky Anti-Virus et ceux qui seront consignés dans le journal des événements. Pour obtenir de plus amples informations sur le journal des événements, consultez le point 13.5 à la page 228.

Les événements liés à l'exécution des tâches sont répartis en trois types selon le degré d'importance : *informatifs*, *importants* et *critiques* :

Evénements informatifs, par exemple *Aucune menace n'a été découverte* ou *Aucune erreur* indiquent les résultats du fonctionnement de Kaspersky Anti-Virus.

Les **Evénements importants** tels que *Erreur de connexion à la source de mise à jour* peuvent avoir un impact sur l'exécution des fonctions de Kaspersky Anti-Virus.

Les **Evénements critiques** peuvent entraîner une violation de la sécurité antivirus du serveur protégé. Il s'agit par exemple des événements *L'intégrité du module a été violée*, *Une menace a été découverte* ou *Erreur interne de la tâche*.

Le niveau de détail des rapports détaillés sur l'exécution des tâches ou du journal des événements correspond au degré d'importance des événements qui y sont consignés. Vous pouvez définir un des trois niveaux de détail depuis **Informatif** où les événements de tous les degrés d'importance sont consignés jusqu'à **Critiques** où seuls les événements critiques sont enregistrés. Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) , pour le composant **Mise à jour**, c'est le niveau **Evénements informatifs** qui est sélectionné.

Vous pouvez également inclure manuellement des événements particuliers dans les événements à consigner dans les rapports détaillés et le journal des événements.

Pour définir le niveau de détail des événements dans les rapports détaillés sur l'exécution des tâches et dans le journal des événements :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Rapports** et sélectionnez **Propriétés**.
2. Dans la boîte de dialogue **Propriétés : Rapports** (cf. ill. 82), liste **Composant**, sélectionnez le composant de Kaspersky Anti-Virus dont vous souhaitez définir le niveau de détail de la tâche.

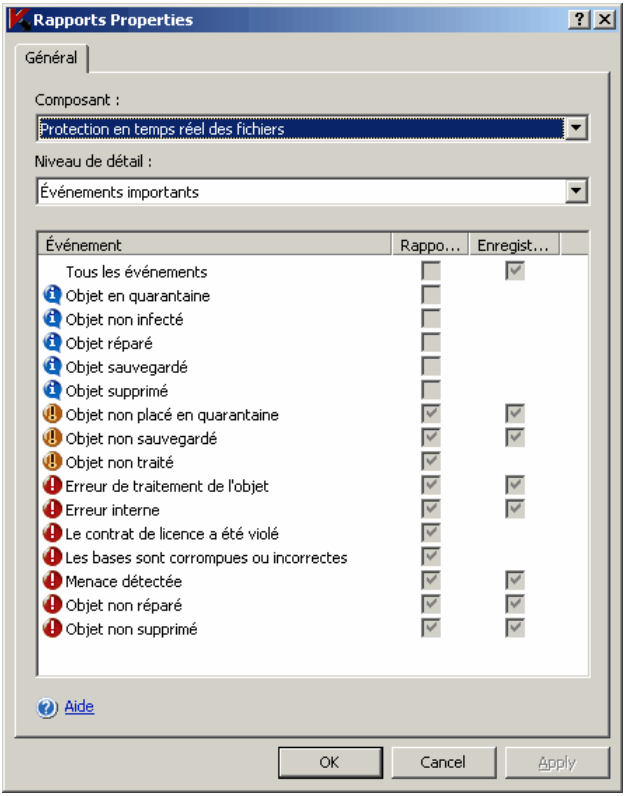

Illustration 82. Boîte de dialogue **Propriétés: Rapports**

3. Exécutez une des actions suivantes :
   - Pour définir le niveau de détail dans les rapports détaillés sur l'exécution des tâches du composant sélectionné, sélectionnez le niveau désiré dans la liste **Niveau de détail**.
     Dans la liste des événements, une case cochée apparaîtra à côté

des événements qui figureront dans les rapports et dans le journal des événements conformément au niveau de détail sélectionné.

- Pour activer l'enregistrement d'événements individuels du composant fonctionnel, dans la liste **Niveau de détail**, sélectionnez **Autre** puis, réalisez les opérations suivantes dans la liste des événements du composant :
  - Pour activer l'enregistrement d'un événement dans les rapports détaillés sur l'exécution des tâches, cochez la case **Rapports** qui lui correspond ; afin de désactiver l'enregistrement d'un événement dans les rapports détaillés, désélectionnez la case **Rapports** qui lui correspond.
  - Pour activer l'enregistrement d'un événement dans le journal des événements, cochez la case **Journal des événements qui lui correspond** ; pour désactiver l'enregistrement d'un événement dans le journal des événements, désélectionnez la case **Journal des événements** qui lui correspond.

4. Cliquez sur **OK**.

13.3. Journal d'audit système

Kaspersky Anti-Virus réalise un audit système des événements liés à l'administration de Kaspersky Anti-Virus tels que le lancement de Kaspersky Anti-Virus, le lancement et l'arrêt des tâches, la modification des paramètres des tâches, la création et la suppression des tâches d'analyse à la demande ou autres. Les enregistrements relatifs à ces événements figurent dans le noeud **Enregistrement d'audit système**.

Par défaut, Kaspersky Anti-Virus conserve les enregistrements dans le journal d'audit système pendant une durée indéterminée. Vous pouvez limiter la durée de conservation des enregistrements à l'aide du paramètre général de Kaspersky Anti-Virus **Durée de conservation des événements dans le journal** d'audit système (cf. point 3.2, p. 46).

Pour consulter les événements dans le journal d'audit système, sélectionnez le noeud **Enregistrement d'audit système** (cf. ill. 83) dans l'arborescence de la console.

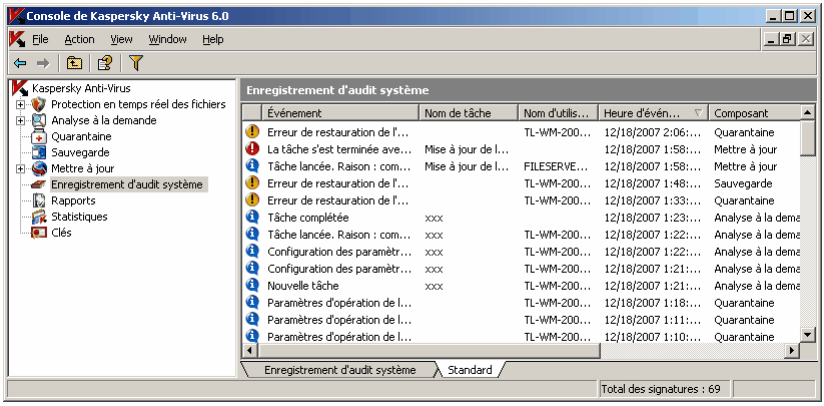

Illustration 83. Noeud **Enregistrement d'audit système**

Le panneau des résultats reprend les informations suivantes sur les événements :

Champ	Description
Événement	Description de l'événement ; inclut le type d'événement et des informations complémentaires à son sujet. Les événements sont classés selon les catégories suivantes en fonction du degré d'importance : *informations*, *importants* ou *critiques*.
Nom de la tâche	Nom de la tâche de Kaspersky Anti-Virus à l'exécution de laquelle l'événement est lié.
Nom d'utilisateur	Si l'événement a été provoqué par un utilisateur de Kaspersky Anti-Virus, alors son nom figure dans cette colonne. Si l'action provient non pas de l'utilisateur mais de Kaspersky Anti-Virus, par exemple la tâche d'analyse à la demande programmée a été lancée, cette colonne affiche l'enregistrement **<domaine><nom de l'ordinateur>$** qui correspond au compte utilisateur **Système local**.
Heure d'événement	Heure d'enregistrement de l'événement selon l'heure du serveur protégé au format défini dans les paramètres régionaux de Microsoft Windows.

Champ	Description
Composant	Composant fonctionnel de Kaspersky Anti-Virus pendant le fonctionnement duquel l'événement s'est produit. Si l'événement n'est pas lié au fonctionnement de composants particuliers mais au fonctionnement de Kaspersky Anti-Virus dans son ensemble, par exemple le lancement de Kaspersky Anti-Virus, alors cette colonne contient l'enregistrement **Application**.
Ordinateur	Nom de l'ordinateur dont l'accès au serveur a été bloqué ou autorisé (uniquement pour la fonction **Blocage de l'accès des ordinateurs**).

Vous pouvez exécuter les actions suivantes sur les événements dans le noeud **Audit système** :

- Trier les événements (cf. point 13.3.1, p. 221) ;
- Filtrer les événements (cf. point 13.3.2, p. 222) ;
- Supprimer les événements (cf. point 13.3.3, p. 223).

13.3.1. Tri des événements dans le journal d'audit système

Par défaut, les événements sont classés dans le noeud **Enregistrement d'audit système** par ordre chronologique inverse.

Pour trouver un événement dans la liste, vous pouvez trier les événements selon le contenu de n'importe laquelle des colonnes. Les résultats du tri sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Enregistrement d'audit système**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour trier les événements :

1. Dans l'arborescence de la console, sélectionnez le noeud **Enregistrement d'audit système**.
2. Dans le panneau des résultats, cliquez sur le titre de la colonne selon laquelle vous souhaitez trier les événements de la liste.

13.3.2. Filtrage des événements dans le journal d'audit système

Pour trouver un événement dans le journal d'audit système, vous pouvez *filtrer les événements*, c.-à-d. afficher dans la liste uniquement les événements qui répondent aux conditions de filtrage que vous aurez définies.

Les résultats du filtrage sont préservés si vous quittez l'écran et ouvrez à nouveau le noeud **Enregistrement d'audit système**, si vous fermez la console de Kaspersky Anti-Virus en l'enregistrant dans un fichier *msc* et que vous ouvrez à nouveau ce fichier.

Pour filtrer les événements dans le journal d'audit système :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Enregistrement d'audit système** et sélectionnez **Filtre**.

   La boîte de dialogue **Paramètres du filtre** s'ouvre (cf. ill. 84).

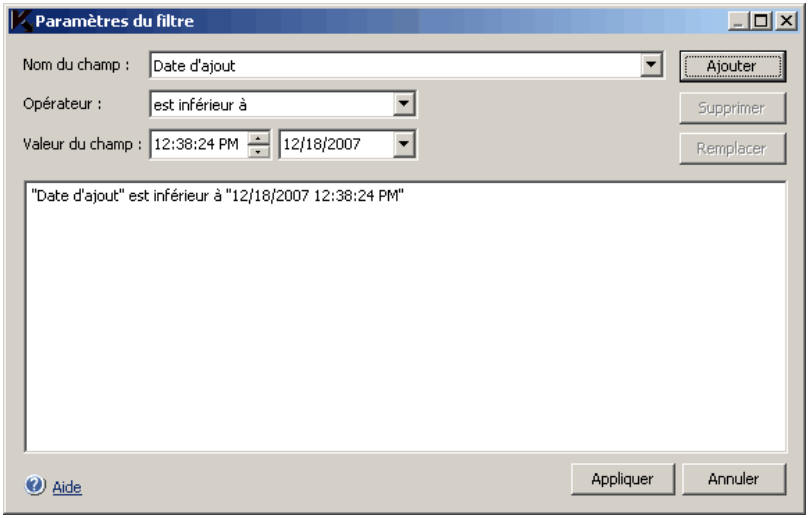

Illustration 84. Boîte de dialogue **Paramètres du filtre**

2. Pour ajouter un filtre :

   a) Dans la liste **Nom du champ**, sélectionnez le champ qui servira pour la comparaison avec la valeur du filtre.

b) Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage peuvent varier en fonction de la valeur sélectionnée dans le champ **Nom du champ**.

c) Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste des valeurs disponibles.

d) Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter. Si vous définissez plusieurs filtres, ils seront unis par le lien logique « ET ».

- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ** puis, cliquez sur le bouton **Remplacer**.

3. Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les événements qui répondent aux conditions des filtres.

*Pour afficher à nouveau tous les événements, dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Enregistrement d'audit système** et sélectionnez **Ôter filtre**.*

13.3.3. Suppression des événements du journal d'audit système

Par défaut, Kaspersky Anti-Virus conservera les événements dans le journal d'audit système pendant une durée indéterminée. Vous pouvez limiter la durée de conservation des événements (cf. configuration du paramètre **Durée de conservation des événements dans le journal** au point 3.2, p. 46).

Vous pouvez supprimer manuellement tous les événements du journal d'audit système.

Pour supprimer tous les événements du journal d'audit système :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Enregistrement d'audit système** et sélectionnez **Purger**.
2. Dans la boîte de dialogue **Confirmation**, cliquez sur le bouton **Oui** afin de confirmer l'opération.

13.4. Statistiques de Kaspersky Anti-Virus

Les statistiques de Kaspersky Anti-Virus reprennent les informations sur l'état actuel de Kaspersky Anti-Virus, de ses composants et des tâches exécutées.

*Pour consulter les statistiques de Kaspersky Anti-Virus, sélectionnez le noeud **Statistiques** dans l'arborescence de la console.*

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

- Lien vers la page en ligne consacrée à Kaspersky Anti-Virus ;
- Version de Kaspersky Anti-Virus et date d'installation ;
- Informations relatives à la clé active : numéro de série, type, date de fin de validité et informations relative à l'expiration prochaine :

  : il reste moins de 14 jours avant l'expiration de la licence

  : il reste moins de 14 avant l'expiration de la licence, mais plus que 7

  : il reste moins de 7 jours avant l'expiration de la licence

  Vous pouvez configurer les notifications de l'administrateur relatives à l'expiration prochaine de la licence (cf. point 15.2, p. 238). Etat et paramètres des composants fonctionnels de Kaspersky Anti-Virus ; état et statistiques des tâches exécutées (cf. description au tableau 15).

Par défaut, les informations du noeud **Statistiques** sont actualisées toutes les minutes. Vous pouvez actualiser les informations du noeud **Statistiques** quand vous le voulez.

*Pour actualiser manuellement les informations dans le noeud **Statistiques**, ouvrez le menu contextuel du noeud **Statistiques** et sélectionnez la commande **Actualiser**.*

Tableau 15. Informations relatives aux composants fonctionnels de Kaspersky Anti-Virus et aux tâches exécutées dans le noeud **Statistiques**

Composant / Tâche	Informations figurant dans le noeud Statistiques
Tâche **Protection en temps réel des fichiers**	Etat de la tâche :  : EN COURS ; la tâche est en cours d'exécution ;  : ARRÊTEE ; la tâche a été arrêtée ou suspendue. Statistiques de la tâche : **Menace découverte** : nombre de menaces découvertes depuis le lancement de la tâche ; **Prévention des épidémies virales** : • **Activé** : le niveau de protection de la tâche **Protection en temps réel des fichiers** a été augmenté» conformément aux paramètres « Prévention des épidémies de virus » (pour obtenir de plus amples informations, lisez le point B.4.4 à la page 419) ; • **Désactivée** : Kaspersky Anti-Virus n'applique pas le mode « Prévention des épidémies virales ». **Objets analysés** : nombre d'objets analysés depuis la dernière exécution de la tâche. Si la tâche **Protection en temps réel des serveurs de fichiers** est exécutée, alors le lien **Détails** ouvre la boîte de dialogue **Statistiques d'exécution de la tâche** (cf. point 0, p. 91).
Interdiction de l'accès des ordinateurs	Etat de l'interdiction automatique de l'accès des ordinateurs :  : la tâche **Protection en temps réel des fichiers** est exécutée et l'interdiction automatique de l'accès des ordinateurs est activée ; le lien **Détails** ouvre la boîte de dialogue **Statistiques** (cf. point 7.9, p. 107) ;  : désactivée. Statistiques de l'interdiction : **Ordinateurs dans la liste d'interdiction d'accès :** nombre d'ordinateurs dans la liste des interdictions à l'heure actuelle

Composant / Tâche	Informations figurant dans le noeud Statistiques
Tâche **Analyse des scripts**	Etat de la tâche :  : EN COURS ; la tâche est en cours d'exécution ;  : ARRÊTEE ; la tâche a été arrêtée ou suspendue. Statistiques de la tâche : **Menace découverte** : nombre de types de menaces découvertes depuis le lancement de la tâche ; **Objets analysés** : nombre de script analysés depuis la dernière exécution de la tâche ; **Scripts interdits** : nombre de script dangereux ou suspects que Kaspersky Anti-Virus a découverts et interdits depuis le lancement de la tâche ; Si la tâche est exécutée, alors le lien **Détails** ouvre la boîte de dialogue **Statistiques d'exécution de la tâche** (cf. point 6.5, p. 95).
État de la base de données	Etat général des bases de Kaspersky Anti-Virus sur le serveur protégé :  : les bases sont d'actualité ;  : les bases de données ne sont plus à jour ;  : la base de données est périmée. Pour obtenir de plus amples informations sur l'actualité des bases, lisez le point 10.1 à la page 152. **Date de création des bases** : date et heure de création des dernières bases actualisées installées ; **Nombre d'enregistrements dans la base** : nombre d'enregistrements dans les bases utilisées pour l'instant.

Composant / Tâche	Informations figurant dans le noeud Statistiques
Quarantaine	L'état général de la quarantaine (affiché si les paramètres **Taille maximale de la quarantaine** et **Seuil d'espace libre en quarantaine** sont appliqués) :  : la taille maximale de la quarantaine n'est pas encore atteinte, le seuil d'espace libre en quarantaine n'est pas encore atteint ;  : la taille maximale de la quarantaine n'est pas encore atteinte, mais bien le seuil d'espace libre en quarantaine ;  : la taille maximale de la quarantaine a été dépassée. Quand le volume de données dans le répertoire de quarantaine atteint les valeurs définies par les paramètres, Kaspersky Anti-Virus alerte l'administrateur (si les notifications pour ces événements ont été configurées). Kaspersky Anti-Virus continue à placer les objets en quarantaine. Pour en savoir plus sur la configuration des notifications, consultez le Chapitre 15 à la page 236. Pour en savoir plus sur la configuration des paramètres de la quarantaine, consultez le point 11.8 à la page 186. Statistiques de quarantaine : **Objets en quarantaine** : nombre d'objets qui se trouvent actuellement en quarantaine ; **Taille** : volume de données dans le répertoire de. Le lien **Détails** ouvre la boîte de dialogue **Statistiques de la quarantaine** (cf. point 11.9, p. 188).

Composant / Tâche	Informations figurant dans le noeud Statistiques
Sauvegarde	L'état général de la quarantaine (affiché si les paramètres **Taille maximale du dossier de sauvegarde** et **Seuil d'espace libre dans le répertoire** sont appliqués) :  : la taille maximale de la sauvegarde n'est pas encore atteinte, le seuil d'espace libre dans la sauvegarde n'est pas encore atteint ;  : la taille maximale de la sauvegarde n'est pas encore atteinte, mais bien le seuil d'espace libre dans la sauvegarde ;  : la taille maximale de la sauvegarde a été dépassée. Quand le volume de données dans la sauvegarde e atteint les valeurs définies par les paramètres, Kaspersky Anti-Virus alerte l'administrateur (si les notifications pour ces événements ont été configurées). Kaspersky Anti-Virus continue à placer les fichiers en sauvegarde. Pour en savoir plus sur la configuration des notifications, consultez le Chapitre 15 à la page 236. Pour en savoir plus sur la configuration des paramètres de la sauvegarde, consultez le point 12.5 à la page 200. Statistiques de sauvegarde : **Nombre d'objets** : nombre d'objets présents actuellement dans la sauvegarde ; **Taille** : volume de données dans la. Le lien **Détails** ouvre la boîte de dialogue **Statistiques de sauvegarde** (cf. point 12.6, p. 202).

13.5. Journal des événements de Kaspersky Anti-Virus dans la console « Event Viewer »

A l'aide de la console MMC Microsoft Windows Event Viewer, vous pouvez consulter le journal des événements de Kaspersky Anti-Virus. Kaspersky Anti-Virus y enregistre les événements importants du point de vue de la sécurité antivirus du serveur protégé et du diagnostic des échecs de Kaspersky Anti-Virus.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements :

- Selon le type d'événement.
- Selon le niveau de détail. Le niveau de détail correspond au niveau d'importance des événements consignés (*Informatifs*, *importants* ou *critiques*). Le niveau le plus détaillé est *Informatif* : les événements de tous les niveaux d'importance sont consignés ; le moins détaillé est le niveau *critique* où seuls les événements critiques sont consignés Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) , pour le composant **Mise à jour**, c'est le niveau **Evénements informatifs** qui est sélectionné.

Pour en savoir plus sur la manière de sélectionner les événements à consigner dans le journal, consultez le point 13.2.7 à la page 217.

Pour consulter le journal des événements :

1. Ajouter le composant enfichable Event Viewer à la console MMC. Si vous administrez la défense du serveur à distance depuis le poste de travail de l'administrateur, désignez le serveur protégé en guise d'ordinateur qui devra être administré via le module enfichable.
2. Dans l'arborescence de la console Event Viewer, ouvrez le noeud **Kaspersky Anti-Virus** (cf. ill. 85).

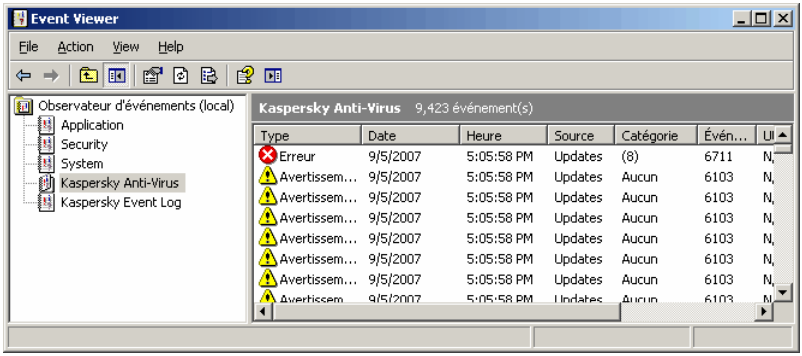

Illustration 85. Informations relatives aux événements de Kaspersky Anti-Virus dans la console « Event Viewer »

CHAPITRE 14. INSTALLATION ET SUPPRESSION DES CLES

Le présent chapitre aborde les sujets suivants :

- Présentation des clés de Kaspersky Anti-Virus (cf. point 14.1, p. 230) ;
- Consultation des informations relatives aux clés installées (cf. point 14.2, p. 232) ;
- Installation d'une clé (cf. point Chapitre 14, p. 230) ;
- Suppression d'une clé (cf. point 14.4, p. 235).

14.1. Présentation des clés de Kaspersky Anti-Virus

La clé est un fichier texte accompagné de l'extension .key. Il contient les informations relatives aux privilèges d'utilisation de Kaspersky Anti-Virus et aux restrictions applicables.

Au moment de diffuser la clé, *la date limite au-delà de laquelle elle ne sera plus valide est définie*(par exemple, le 31 décembre 2010 si la clé a été diffusée en 2007) et la *période de validité de la clé* en jours (par exemple, 365 jours) est également définie. Kaspersky Lab peut distribuer des clés dont les périodes de validité diffèrent.

Lors de l'installation de la clé, Kaspersky Anti-Virus calcule *la date de fin de validité de la clé* : cette date correspond à la fin de la période de validité à partir de l'installation de la clé mais ne peut être postérieure à la date après laquelle la clé devient invalide. Pendant cette période, vous avez accès aux possibilités suivantes :

- Protection antivirus ;
- Maintient de l'actualité des bases (mises à jour des bases) ;
- Réception des mises à jour urgentes des modules de Kaspersky Anti-Virus (patch) ;
- Installation des mises à jour prévues de Kaspersky Anti-virus (mises à niveau).

Pendant cette période, Kaspersky Lab ou son partenaire vous offre une assistance technique pour autant que celle-ci soit prévue dans les conditions de la clé.

Une fois la *date de fin de validité de la clé* passée, Kaspersky Anti-Virus arrête d'exécuter ses fonctions : en fonction du type de clé vous ne pourrez plus utiliser soit les fonctions de mise à jour des bases et des modules de Kaspersky Anti-Virus et l'assistance technique, soit toutes les fonctions de Kaspersky Anti-Virus.

Il existe trois types de clé pour Kaspersky Anti-Virus : *test bêta*, *évaluation* et *commerciale.*

Clé pour test bêta

La clé pour test bêta est offerte gratuitement. Elle est proposée uniquement durant les tests bêta de Kaspersky Anti-Virus. Une fois que la clé est parvenue à échéance, toutes les fonctions de Kaspersky Anti-Virus sont désactivées.

Clé d'évaluation

La clé d'évaluation est également proposée gratuitement. Elle permet aux utilisateurs de découvrir Kaspersky Anti-Virus. La durée de validité d'une clé d'évaluation n'est pas très longue ; à la fin de celle-ci, toutes les fonctions de Kaspersky Anti-Virus sont désactivées. Vous pouvez installer uniquement une clé d'évaluation de Kaspersky Anti-Virus.

Clé commerciale.

Une fois que la clé commerciale est arrivée à échéance, Kaspersky Anti-Virus continue à fonctionner, à l'exception de la mise à jour. L'analyse du serveur s'opère à l'aide des bases installée avant la date de fin de validité de la clé. Il n'identifie pas les menaces ajoutées aux bases par les experts de Kaspersky Lab après la fin de la validité de la clé et il ne répare par les objets infectés par ces menaces. L'assistance technique est également offerte uniquement durant la période de validité de la clé.

Vous pouvez acheter et installer directement deux clés : une clé en guise de clé active et l'autre, en guise de clé de réserve. La clé *active* entre en fonction dès son installation tandis que la clé de *réserve* entre en fonction automatiquement dès que la clé active est parvenue à échéance.

La clé de Kaspersky Anti-Virus peut imposer des restrictions d'utilisation en fonction du nombre de serveurs.

14.2. Consultation des informations relatives aux clés installées

Pour consulter les informations relatives aux clés installées :

1. Dans l'arborescence de la console, sélectionnez le noeud **Clés de licence**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur la clé dont vous souhaitez consulter les données et sélectionnez **Propriétés**.

   La boîte de dialogue **Propriétés: <numéro de série de la clé>** s'ouvre (cf. ill. 86).

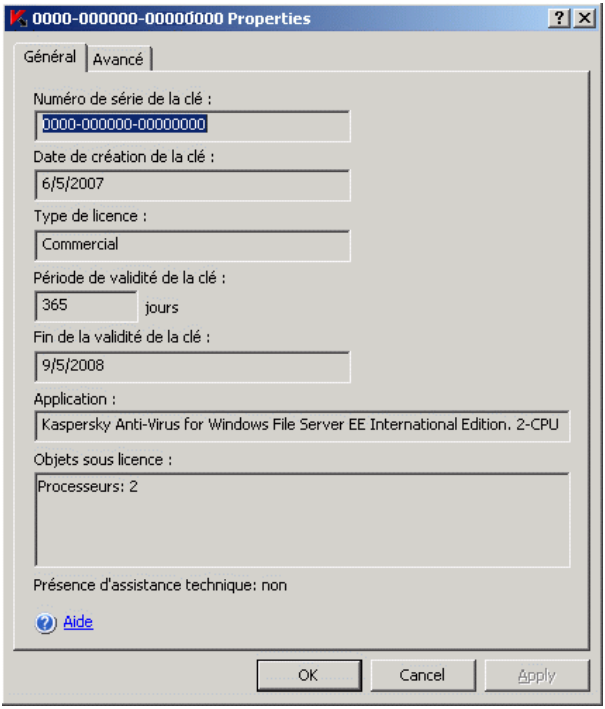

Illustration 86. Boîte de dialogue **Propriétés de la clé**, onglet **Général**

Dans la boîte de dialogue **Propriétés: <numéro de série de la clé>**, onglet **Général**, vous pourrez lire les informations suivantes :

Tableau 16. Information sur la clé

Champ	Description
Numéro de série de la clé	Numéro de série de la clé
Date de création de la clé	Date de délivrance de la clé
Type de licence	Type de clé (test bêta, évaluation ou commerciale). Pour obtenir de plus amples informations sur les types de clé, lisez le point 14.1 à la page 230.
Période de validité de la clé	Période d'activité de la clé (en jours), définie au moment de son attribution
Fin de la validité de la clé	Date de fin de validité de la clé ; déterminée par Kaspersky Anti-Virus lors de l'installation de la clé ; correspond à la fin de la *période de validité* de la clé depuis son activation mais elle ne peut être ultérieure à la *date à laquelle la clé n'est plus valide*
Application	Nom de Kaspersky Anti-Virus
Objets sous licence	Restrictions prévues par la clé de licence (le cas échéant)
Présence d'assistance technique	Indique si la clé prévoit une assistance technique offerte par Kaspersky Lab ou par ses partenaires

Dans la boîte de dialogue **Propriétés: <numéro de série de la clé>**, onglet **Avancé**, vous pourrez lire les informations relatives au client ainsi que les coordonnées de Kaspersky Lab ou du distributeur où vous avez acheté Kaspersky Anti-Virus.

14.3. Installation de la clé

Pour installer la clé :

1. Dans l'arborescence de la console, ouvrez le menu contextuel du noeud **Clés** et sélectionnez **Installer la licence**.
2. Dans la boîte de dialogue **Installer la licence** (ill. 87), indiquez le nom du fichier de la licence et son chemin d'accès.

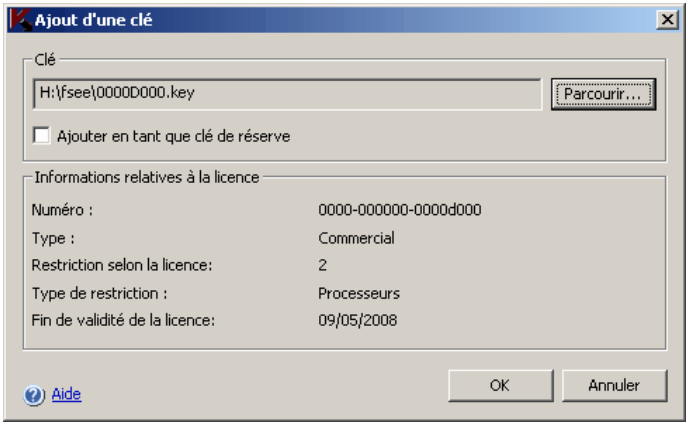

Illustration 87. Boîte de dialogue **Ajout d'une clé**

La boîte de dialogue reprend les informations relatives à la licence décrites dans le tableau ci-après.

3. Si vous installez la clé en tant que clé de réserve, alors cochez la case **Ajouter en tant que clé de réserve**.
4. Cliquez sur **OK**.

La boîte de dialogue **Installer la licence** reprend les informations suivantes sur la clé installée :

Tableau 17. Information sur la clé

Champ	Description
Numéro	Numéro de série de la clé
Type	Type de clé (test bêta, évaluation ou commerciale). Pour obtenir de plus amples informations sur les types de clé, lisez le point 14.1 à la page 230.
Restriction selon la licence	Nombre d'objets limités
Type de restriction	Objets limités

Champ	Description
Fin de validité de la licence	Date de fin de validité de la licence ; déterminée par Kaspersky Anti-Virus ; correspond à la fin de la période de validité de la clé *depuis son activation* mais elle ne peut être ultérieure *à la date à laquelle la clé n'est plus valide*. Pour de plus amples informations, consultez le point 14.1 à la page 230.

14.4. Suppression de la clé

Vous pouvez supprimer une clé installée.

Si vous supprimez une clé active lors de l'installation de la clé de réserve, la clé de réserve deviendra automatiquement active.

Attention !

Si vous supprimez une clé installée, vous pouvez la rétablir en la réinstallant depuis le fichier de clé.

Pour supprimer la clé installée :

1. Dans l'arborescence de la console, sélectionnez le noeud **Clés**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations sur la clé que vous souhaitez supprimer et sélectionnez **Supprimer la licence**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

CHAPITRE 15. CONFIGURATION DES NOTIFICATIONS

Le présent chapitre aborde les sujets suivants :

- Moyens de notification de l'administrateur et des utilisateurs (cf. point 15.1, p. 236) ;
- Configuration des notifications (cf. point 15.2, p. 238).

15.1. Moyens de notification de l'administrateur et des utilisateurs

Kaspersky Anti-Virus permet d'alerter l'administrateur et les utilisateurs qui accèdent au serveur protégé au sujet des événements liés au fonctionnement de Kaspersky Anti-Virus et à l'état de la protection antivirus du serveur :

- L'administrateur peut obtenir des informations sur les événements de certains types ;
- Les utilisateurs du réseau local qui accèdent au serveur protégé peuvent obtenir des informations sur les événements de type *Menace découverte* et *L'ordinateur a été ajouté à la liste d'interdiction* ; les utilisateurs du serveur via le terminal peuvent obtenir des informations sur les événements *Une menace a été découverte*.

Vous pouvez, dans la console MMC de Kaspersky Anti-Virus, configurer les notifications de l'administrateur et des utilisateurs de diverses manières. Ces méthodes sont décrites dans les tableaux ci-après.

Tableau 18. Moyens de notification des utilisateurs

Moyen de notification	Configuration par défaut	Description
Fenêtre des services des terminaux	Configuré selon les événements de type *Une menace a été découverte*	Si le serveur protégé est terminal, vous pouvez appliquer cette méthode afin d'alerter les utilisateurs via terminal.
Fenêtre du service de messagerie de Microsoft Windows	Configuré en fonction des événements du type *Une menace a été découverte* et *L'ordinateur a été ajouté à la liste d'interdiction*	Ce mode utilise le service de messagerie de Microsoft Windows. Avant d'opter pour ce mode, assurez-vous que le service de messagerie est activé sur le serveur protégé et sur les postes de travail des utilisateurs du réseau local (il est désactivé par défaut).

Tableau 19. Moyens de notification des administrateurs

Moyen de notification	Configuration par défaut	Description
Notification via le service de messagerie de Microsoft Windows	Non configuré	Ce mode de notification utilise le service de messagerie de Microsoft Windows. Avant d'opter pour ce mode de notification, assurez-vous que le service de messagerie est activé sur le serveur protégé et sur l'ordinateur qui fait office de poste de travail de l'administrateur (si l'administrateur administre Kaspersky Anti-Virus à distance). Le service de messagerie est désactivé par défaut.
Lancement du fichier exécutable	Non configuré	Ce mode de notification lance le fichier exécutable indiqué quand un événement défini survient. Le fichier exécutable doit se trouver sur le disque local du serveur protégé.

Moyen de notification	Configuration par défaut	Description
Notification par courrier électronique	Non configuré	Ce mode transmet les notifications via le courrier électronique.

Vous pouvez créer un texte différent pour chaque type d'événement. Ce texte peut contenir des champs avec les informations sur l'événement.

Le texte du message utilisé par défaut pour la notification des utilisateurs est repris dans le tableau suivant.

Tableau 20. Texte du message composé par défaut pour la notification des utilisateurs

Tâche	Type d'événement	Texte du message
Protection en temps réel des fichiers	*Menace détectée*	Kaspersky Anti-Virus a bloqué l'accès à %OBJECT% sur l'ordinateur %FROM_COMPUTER% à %EVENT_TIME%. Cause : %EVENT_TYPE%. Type de menace : %VIRUS_TYPE%: %VIRUS_NAME%. Utilisateur de l'objet : %USER_NAME%. Nom du poste de l'utilisateur de l'objet : %USER_COMPUTER%
Protection en temps réel des fichiers, fonction *Interdiction de l'accès des ordinateurs*	*L'ordinateur a été ajouté à la liste d'interdiction*	Kaspersky Anti-Virus sur l'ordinateur %FROM_COMPUTER%: %EVENT_TYPE%. Nom de poste : %USER_COMPUTER%. Heure d'interdiction : %EVENT_TIME%. Cause : tentative d'écriture de fichiers infectés ou suspects. Contactez l'administrateur système de votre réseau

15.2. Configuration des notifications

La configuration des notifications sur les événements porte sur le mode de notification et sur la composition du texte du message.

Pour configurer les notifications sur les événements :

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

   La boîte de dialogue **Notifications** s'ouvre (cf. ill. 88).

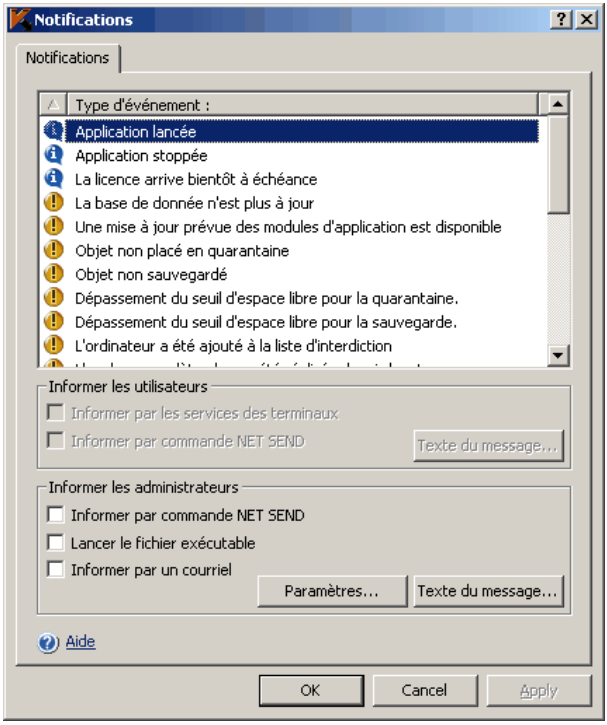

Illustration 88. Boîte de dialogue **Notifications**

2. Dans la boîte de dialogue **Notifications**, onglet **Notifications**, sélectionnez les événements et définissez le mode de notification pour ceux-ci :

   - Pour définir les moyens de notification de l'administrateur, réalisez les actions suivantes :

     a) Dans la liste **Type d'événement**, sélectionnez les types d'événements (*Menace découverte* et *l'ordinateur a été ajouté à la liste des interdictions*) au sujet desquels vous souhaitez prévenir les utilisateurs sur les ordinateurs où ces événements se produisent ;

b) Dans le groupe de paramètres **Informer les administrateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

- Pour définir les moyens de notification des utilisateurs, réalisez les actions suivantes :

  a) Dans la liste **Type d'événement**, sélectionnez l'événement dont vous souhaitez configurer la notification ;

  b) Dans le groupe de paramètres **Informer les utilisateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

> **Remarque**
>
> Vous pouvez composer un message pour plusieurs types d'événement : après avoir choisi le mode de notification pour un type d'événement, sélectionnez les autres événements pour lesquels vous souhaitez utiliser le même message en appuyant sur la touche **<Ctrl>** ou **<Shift>**.

3. Pour composer le texte du message, cliquez sur le bouton **Texte du message** dans le groupe de paramètres requis et dans la boîte de dialogue **Texte du message**, saisissez le texte qui apparaîtra dans les notifications relatives aux événements.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Macro** et sélectionnez les champs désirés dans la liste. Les champs avec les informations sur les événements sont repris au Tableau 21.

   Pour revenir au texte prévu par défaut pour l'événement, cliquez sur le bouton **Par défaut**.

4. Pour configurer les modes de notifications de l'administrateur sur les événements sélectionnés, cliquez sur le bouton **Paramètres avancés** et dans la boîte de dialogue **Notifications**, procédez à la configuration des modes sélectionnés.

   - Pour les notifications via courrier électronique, ouvrez l'onglet **Courriel** (cf. ill. 89) et dans les champs prévus à cet effet, saisissez l'adresse électronique du destinataire (séparez les adresses par un point virgule), le nom ou l'adresse de réseau du serveur SMTP ainsi que son port. Si nécessaire, indiquez le texte qui figurera dans les champs **Objet** et **De** le texte du champ **Objet** peut contenir des valeurs de champs d'informations (cf. Tableau 21).

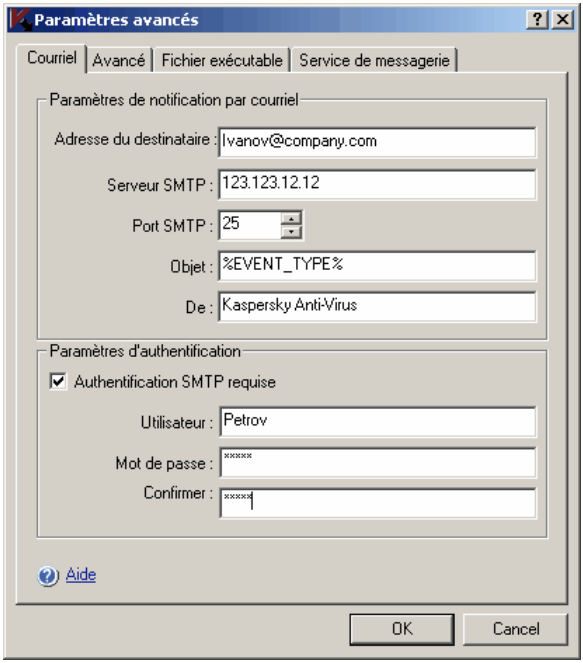

Illustration 89. Boîte de dialogue **Paramètres avancés**, onglet **Courriel**

Si vous souhaitez utiliser la vérification de l'authenticité selon le compte utilisateur lors de la connexion au serveur SMTP, il faudra dans ce cas cochez la case **Authentification SMTP requise** dans le groupe **Paramètres d'authentification** et saisir le nom et le mot de passe de l'utilisateur dont l'authenticité sera vérifiée.

- Pour les notifications via le service de messagerie, composez la liste des ordinateurs qui recevront les messages dans l'onglet **Service de messagerie** (cf. ill. 90) : pour chaque ordinateur que vous souhaitez ajouter, cliquez sur le bouton **Ajouter** et saisissez son nom de réseau dans le champ. N'indiquez pas l'adresse IP de l'ordinateur dans ce champ.

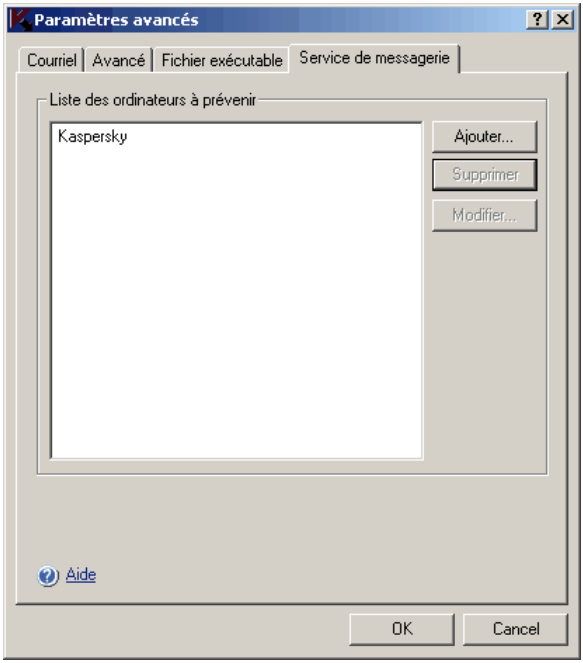

Illustration 90. Boîte de dialogue **Paramètres avancés**, onglet **Service de messagerie**

- Pour le lancement d'un fichier exécutable, sélectionnez le fichier sur le disque local du serveur protégé qui sera exécuté sur le serveur lorsque l'événement se produira dans l'onglet **Fichier exécutable** (cf. ill. 91) ou saisissez le chemin d'accès à ce dernier. Saisissez le nom et le mot de passe de l'utilisateur sous le compte duquel le fichier sera exécuté.

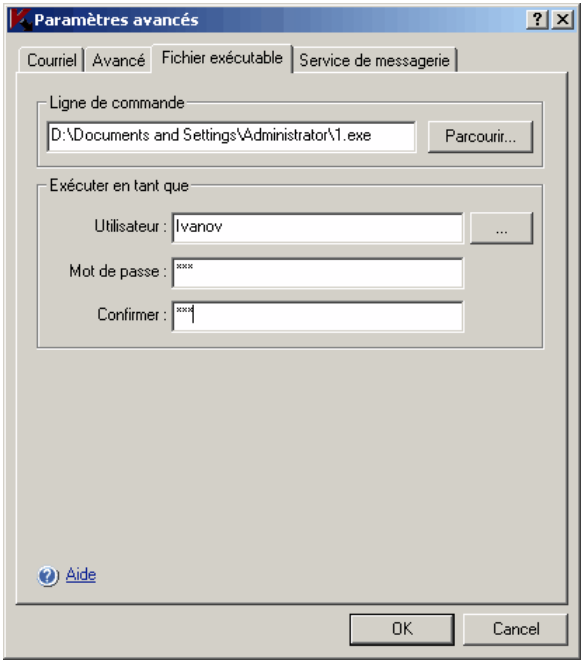

Illustration 91. Boîte de dialogue **Paramètres avancés**, onglet **Fichier exécutable**

- Si vous souhaitez limiter le nombre de messages en fonction d'événement d'un même type par unité de temps, cochez la case **Ne pas répéter la notification plus de** sur l'onglet **Avancé** (cf. ill. 92) et indiquez la valeur souhaitée par unité de temps.

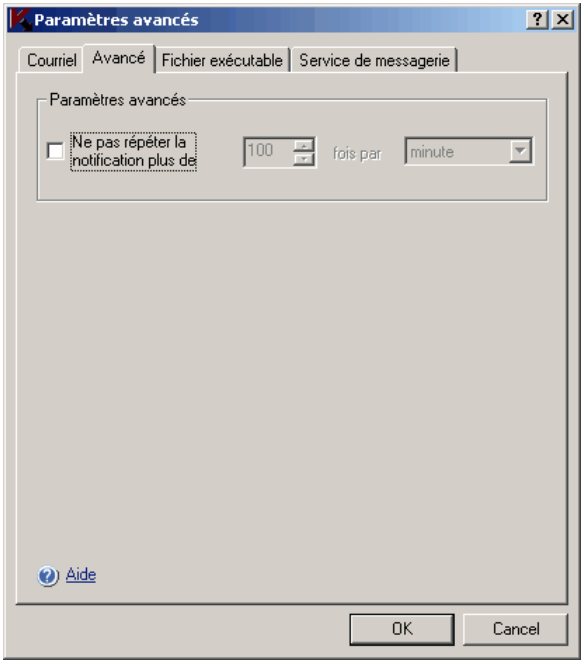

Illustration 92. Boîte de dialogue **Paramètres avancés**, onglet **Avancé**

5. Cliquez sur **OK**.

Tableau 21. Champs d'information sur les événements

Champ	Description
%EVENT_TYPE%	Type d'événement
%EVENT_TIME%	Heure à laquelle l'événement s'est produit
%EVENT_SEVERITY%	Degré d'importance de l'événement
%OBJECT%	Nom de l'objet (dans les tâches de protection en temps réel et d'analyse à la demande). Dans la tâche **Mise à jour des modules de l'application**, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.

Champ	Description
%VIRUS_NAME%	Nom de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande)
%VIRUS_TYPE%	Type de la menace selon le classement de Kaspersky Lab ; fait partie du nom complet de la menace que Kaspersky Anti-Virus renvoie (dans les tâches de protection en temps réel et d'analyse à la demande)
%USER_COMPUTER%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'ordinateur dont l'utilisateur a sollicité un objet sur le serveur
%USER_NAME%	Dans la tâche **Protection en temps réel des fichiers**, il s'agit du nom de l'utilisateur qui a sollicité un objet sur le serveur
%FROM_COMPUTER%	Nom du serveur protégé d'où provient la notification
%REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements)
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement *erreur interne de la tâche*)
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)

PARTIE 2. ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA LA LIGNE DE COMMANDE

Cette section aborde les sujets suivants :

- Description de l'administration de Kaspersky Anti-Virus via la ligne de commande (cf. Chapitre 16, p. 247) ;
- Description des codes de retour (cf. Chapitre 17, p. 270).

CHAPITRE 16. ADMINISTRATION DE KASPERSKY ANTI-VIRUS VIA LA LIGNE DE COMMANDE

Vous pouvez réaliser les principales opérations d'administration de Kaspersky Anti-Virus via la ligne de commande du serveur protégé pour autant que le composant **Utilitaire de ligne de commande** ait été inclus dans la liste des composants à installer pendant l'installation de Kaspersky Anti-Virus.

La ligne de commande vous permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Anti-Virus (pour de plus amples informations sur les privilèges d'accès aux fonctions de Kaspersky Anti-Virus, lisez le point 2.6.1 à la page 39).

Certaines des commandes de Kaspersky Anti-Virus sont exécutées en mode synchrone : l'administration revient à la console uniquement après la fin de l'exécution de la commande ; d'autres commandes sont exécutées en mode asynchrone : l'administration revient à la console directement après le lancement de la commande.
Pour interrompre l'exécution d'une commande en mode asynchrone, appuyez sur la combinaison de touches <**Ctrl+C**>.
Lors de la saisie d'une commande de Kaspersky Anti-Virus, respectez les règles suivantes :

- Saisissez les paramètres et les commandes en majuscules ou en minuscules ;
- Séparez les paramètres par des espaces ;
- Si le nom du fichier attribué en tant que valeur d'un paramètre contient un espace, alors saisissez ce nom (et son chemin d'accès) entre guillemets, par exemple : “C:\TEST\test cpp.exe” ;
- Dans les masques des noms des fichiers ou des chemins, utilisez uniquement un caractère de remplacement et saisissez-le à la fin du chemin d'accès au répertoire ou au fichier, par exemple : "C:\Temp\Temp*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc".

La liste des commandes de Kaspersky Anti-Virus est reprise au tableau 22.
Les codes de retour des commandes de Kaspersky Anti-Virus sont repris au Chapitre 17 à la page 270.

Tableau 22. Commandes de Kaspersky Anti-Virus

Commande	Description
KAVSHELL HELP (16.1)	Affiche l'aide sur les commandes de Kaspersky Anti-Virus
KAVSHELL START (16.2)	Lance le service de Kaspersky Anti-Virus
KAVSHELL STOP (16.2)	Arrête le service de Kaspersky Anti-Virus
KAVSHELL SCAN (16.3)	Crée et lance une tâche d'analyse à la demande temporaire dont la couverture d'analyse et les paramètres de sécurité sont définis par les paramètres de la commande
KAVSHELL FULLSCAN (16.4)	Lance la tâche prédéfinie **Analyse complète de l'ordinateur**
KAVSHELL TASK (16.5)	Lance/suspend/relance/arrête la tâche indiquée en mode asynchrone/donne l'état actuelle de la tâche et les statistiques de la tâche
KAVSHELL RTP (16.6)	Lance et arrête toutes les tâches de protection en temps réel
KAVSHELL UPDATE (16.7)	Lance la tâche de mise à jour des bases de Kaspersky Anti-Virus selon les paramètres définis à l'aide des arguments de la ligne de commande
KAVSHELL ROLLBACK (16.8)	Remet les bases à l'état antérieur à la mise à jour
KAVSHELL LICENSE (16.9)	Gère les clés de licence
KAVSHELL TRACE (16.10)	Active ou désactive la création du fichier de traçage, gère les paramètres du fichier de traçage
KAVSHELL DUMP (16.11)	Active ou désactive la création d'un vidage de mémoire des processus de Kaspersky Anti-Virus en cas d'arrêt suite à une erreur
KAVSHELL IMPORT (16.12)	Importe les paramètres généraux de Kaspersky Anti-Virus, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration créé au préalable

Commande	Description
KAVSHELL EXPORT (16.13)	Exporte tous les paramètres de Kaspersky Anti-Virus et des tâches existantes dans un fichier de configuration

16.1. Affichage de l'aide sur les commandes de Kaspersky Anti-Virus. KAVSHELL HELP

Pour obtenir la liste de toutes les commandes de Kaspersky Anti-Virus, saisissez une des commandes suivantes :

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une commande, saisissez une des commandes suivantes :

```
KAVSHELL HELP <commande>
KAVSHELL <commande> /?
```

Exemples de commande KAVSHELL HELP

`KAVSHELL HELP SCAN` : consultation des informations détaillées sur la commande KAVSHELL SCAN.

16.2. Lancement et arrêt du service de Kaspersky Anti-Virus. KAVSHELL START, KAVSHELL STOP

Pour lancer le service de Kaspersky Anti-Virus, utilisez la commande KAVSHELL START.

Remarque

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

Pour arrêter le service de Kaspersky Anti-Virus, utilisez la commande KAVSHELL STOP.

16.3. Analyse du secteur indiqué. KAVSHELL SCAN

Pour lancer la tâche d'analyse de secteurs définis du serveur protégé, utilisez la commande KAVSHELL SCAN. Les arguments de cette commande définissent les paramètres de la tâche (couverture d'analyse et paramètres de sécurité).

La tâche d'analyse à la demande lancée à l'aide de la commande KAVSHELL SCAN est *temporaire*. Elle apparaît dans la console de Kaspersky Anti-Virus dans MMC uniquement pendant son exécution (la console de Kaspersky Anti-Virus ne vous permet pas de consulter les paramètres de la tâche). Le rapport sur l'exécution de la tâche est crée en même temps ; il apparaît dan le noeud **Rapports** de la console de Kaspersky Anti-Virus. A l'instar des tâches d'analyse à la demande créées dans la console de Kaspersky Anti-Virus, les tâches créées et lancées à l'aide de la commande SCAN peuvent être soumises à la stratégie de l'application Kaspersky Administration Kit (pour de plus amples informations sur l'utilisation de Kaspersky Administration Kit dans l'administration de Kaspersky Anti-Virus, lisez le Partie 3 à la page 276).

La commande KAVSHELL SCAN est exécutée en mode synchrone.

Pour lancer une tâche d'analyse à la demande existante depuis la ligne de commande, utilisez la commande KAVSHELL TASK (cf. point 16.5, page 256).

Syntaxe de la commande KAVSHELL SCAN

```
KAVSHELL SCAN <couverture d'analyse>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:< nom du fichier avec la liste des couvertures d'ana-
lyse >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE]
[/E:<ABMSPO>] [/EM:<”masque”>] [/ES:<taille>] [/ET:<nombre
de seconde>] [/NOICHECKER][/NOISWIFT][/W:<nom du fichier du
rapport>] [/ALIAS:<nom alternatif de la tâche>]
```

Exemples de commande KAVSHELL SCAN

```
KAVSHELL SCAN Folder4 D:\Folder1\Folder2\Folder3\
C:\Folder1\ C:\Folder2\3.exe "\\server1\Shared Folder\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.ff?;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:report.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:report.log
```

Argument	Description
Couverture de l'analyse. Argument obligatoire.	
<fichiers>	Couverture d'analyse : liste des fichiers, des répertoires, des chemins de réseau et des secteurs prédéfinis. Indiquez les chemins de réseau au format UNC (Universal Naming Convention). Dans l'exemple suivant, le répertoire Folder4 est indiqué sans son chemin d'accès. Il se trouve dans le répertoire d'où la commande KAVSHELL est exécutée : KAVSHELL SCAN Folder4
<répertoires>	
<chemin de réseau>	
/MEMORY	Analyser les objets dans la mémoire vive
/SHARED	Analyser les dossiers partagés sur le serveur
/STARTUP	Analyser les objets de démarrage
/REMDRIVES	Analyser les disques amovibles
/FIXDRIVES	Analyser les disques durs
/MYCOMP	Analyser tous les secteurs du serveur protégé

Argument	Description

/L: <nom du fichier avec la liste des couvertures d'analyse>	Nom du fichier avec la liste des couvertures d'analyse, y compris le chemin d'accès complet au fichier.
	Les couvertures d'analyse dans le fichier sont séparées par un « retour à la ligne » Vous pouvez indiquer les couvertures d'analyse prédéfinies comme indiquer dans l'exemple si après de fichier avec la liste des couvertures d'analyse :
	`C:\`
	`D:\Docs\*.doc`
	`E:\My Documents`
	`/STARTUP`
	`/SHARED`

Objets à analyser (File types). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus analysera les objets en fonction du format.	
/FA	Analyser tous les objets
/FC	Analyser les objets en fonction du format (par défaut). Kaspersky Anti-Virus analyse uniquement les objets dont le format figure dans la liste des formats propres aux objets pouvant être infectés.
/FE	Analyser les objets en fonction de l'extension. Kaspersky Anti-Virus analyse uniquement les objets dont l'extension figure dans la liste des extensions propres aux objets pouvant être infectés.
/NEWONLY	Analyser uniquement les objets neufs ou modifiés (pour en savoir plus sur ce paramètre, consultez le point B.3.2 à la page 400). Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus analysera tous les objets.
/AI: **Actions à exécuter sur les objets infectés**. Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus appliquera l'action **Ignorer**.	
DISINFECT	Réparer, ignorer si la réparation est impossible
DISINFDEL	Réparer, supprimer si la réparation est impossible
DELETE	Supprimer
REPORT	Ignorer (par défaut)

Argument	Description
AUTO	Exécuter l'action recommandée
/AS: **Actions à exécuter sur les objets suspects** (actions). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Anti-Virus appliquera l'action **Ignorer**.	
QUARANTINE	Quarantaine
DELETE	Supprimer
REPORT	Ignorer (par défaut)
AUTO	Exécuter l'action recommandée
Exclusions	
/E:ABMSPO	L'argument exclut les objets composés des types suivants : A : archives ; B : bases de données de messagerie électronique ; M : message de texte plat ; S : archives SFX ; P : objets compactés ; O : objets OLE intégrés.
/EM:<"masque">	Exclure les fichiers en fonction du masque. Vous pouvez définir plusieurs masques, par exemple : EM:"*.txt;*.pn?; C\Videos*.avi".
/ET:<nombre de secondes>	Arrêter le traitement de l'objet s'il dure plus longtemps que la durée indiquée en secondes. Par défaut, l'analyse n'est pas limitée dans le temps.
/ES:<taille>	Exclut de l'analyse les objets composés dont la taille, en mégaoctets, dépasse la valeur de l'argument <taille>. Par défaut, Kaspersky Anti-Virus analyse les objets de n'importe quelle taille.
Paramètres complémentaires (Options)	

Argument	Description
/NOICHECKER	Désactive l'utilisation de la technologie iChecker (activée par défaut).
/NOISWIFT	Désactive l'utilisation de la technologie iSwift (activée par défaut).
/ALIAS:<nom alternatif de la tâche>	L'argument permet d'attribuer un nom temporaire à la tâche d'analyse à la demande. Ce nom permet de consulter la tâche durant son exécution, par exemple pour consulter les statistiques à l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Anti-Virus. Si l'argument n'est pas défini, alors la tâche reçoit le nom alternatif scan_<kavshell_pid>, par exemple, scan_1234. Dans la console de Kaspersky Anti-Virus, la tâche reçoit le nom Scan objects (<date et heure>), par exemple, Scan objects 8/16/2007 5:13:14 PM.
Paramètres des rapports (Report settings)	

Argument	Description
/W:<nom du fichier du rapport>	Si vous définissez cet argument, Kaspersky Anti-Virus enregistre le fichier de rapport sur la tâche et lui donne le nom défini par l'argument. Le fichier du rapport contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le rapport reprend les événements définis par les paramètres des rapports et du journal des événements dans la console Kaspersky Anti-Virus (pour de plus amples informations, lisez le point 13.2.7 à la page 217). Vous pouvez indiquer un chemin absolu ou relatif au fichier du rapport. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier sera créé dans le répertoire en cours. Un nouveau lancement de la commande selon les mêmes paramètres de consignation écrase le rapport existant. Vous pouvez consulter le fichier du rapport durant l'exécution de la tâche. Le rapport sur la tâche figure dans le noeud **Rapports** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de rapport, il n'interrompt pas l'exécution de la commande et n'affiche pas de message sur l'erreur.

16.4. Lancement de la tâche *Analyse complète de l'ordinateur.* KAVSHELL FULLSCAN

Utilisez la commande KAVSHELL FULLSCAN, pour lancer la tâche prédéfinie d'analyse à la demande **Analyse complète de l'ordinateur** selon les paramètres définis dans la console de Kaspersky Anti-Virus dans MMC.

Syntaxe de la commande KAVSHELL FULLSCAN

```
KAVSHELL FULLSCAN [/W:<nom du fichier du rapport>]
```

Exemples de la commande KAVSHELL FULLSCAN

`KAVSHELL FULLSCAN /W:fullscan.log` : exécute l'analyse à la demande **Analyse complète de l'ordinateur** ; le rapport sur les événements de la tâche est conservé dans le fichier fullscan.log du répertoire en cours.

Argument	Description
/W:<nom du fichier du rapport>	Si vous désignez cet argument, Kaspersky Anti-Virus enregistre le fichier de rapport sur la tâche et lui donne le nom défini par l'argument. Le fichier du rapport contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le rapport reprend les événements définis par les paramètres des rapports et du journal des événements dans la console Kaspersky Anti-Virus (pour de plus amples informations, lisez le point 13.2.7 à la page 217). Vous pouvez indiquer un chemin absolu ou relatif au fichier du rapport. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du rapport sera créé dans le répertoire en cours. Un nouveau lancement de la commande selon les mêmes paramètres de consignation écrase le fichier de rapport existant. Le rapport sur la tâche figure dans le noeud **Rapports** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de rapport, il n'interrompt pas l'exécution de la commande et n'affiche pas de message sur l'erreur.

16.5. Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK

A l'aide de la commande KAVSHELL TASK, vous pouvez administrer la tâche indiquée : lancer, suspendre, reprendre ou arrêter la tâche ainsi que consulter son état actuel et ses statistiques. La commande est exécutée en monde asynchrone.

Syntaxe de la commande KAVSHELL TASK

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP
| /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemples de la commande KAVSHELL TASK

```
KAVSHELL TASK
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-computer /STATE
```

Argument	Description
Sans argument	La commande renvoie la liste de toutes les tâches existantes de Kaspersky Anti-Virus. La liste contient les champs : nom alternatif de la tâche, catégorie de tâche (tâche prédéfinie, tâche définie par utilisateur et tâche de groupe) et état actuel de la tâche.
<nom alternatif de la tâche>	Au lieu du nom de la tâche dans la commande SCAN TASK, utilisez son nom alternatif : bref nom complémentaire attribué aux tâches par Kaspersky Anti-Virus. Pour consulter les noms alternatifs des tâches dans Kaspersky Anti-Virus, saisissez la commande KAVSHELL TASK sans argument.
/START	Lance la tâche indiquée en mode asynchrone
/STOP	Arrête la tâche indiquée
/PAUSE	Suspend la tâche indiquée
/RESUME	Relance la tâche indiquée en mode asynchrone
/STATE	Donne l'état actuel de la tâche (*En cours, Terminée, Pause, Terminée sur une erreur, Lancée, Relancée*))
/STATISTICS	Affiche les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche jusqu'à ce moment.

16.6. Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP

La commande KAVSHELL RTP vous permet de lancer ou d'arrêter toutes les tâches de protection en temps réel.

Syntaxe de la commande KAVSHELL RTP

`KAVSHELL RTP </START | /STOP>`

Exemples de la commande KAVSHELL RTP

`KAVSHELL RTP /START` : lance toutes les tâches de protection en temps réel.

Argument	Description
/START	Lance toutes les tâches de protection en temps réel
/STOP	Arrête toutes les tâches de protection en temps réel

16.7. Lancement de la tâche de mise à jour des bases de Kaspersky Anti-Virus. KAVSHELL UPDATE

La commande KAVSHELL UPDATE vous permet de lancer la tâche de mise à jour des bases de Kaspersky Anti-Virus en mode synchrone.
La tâche de mise à jour des bases de Kaspersky Anti-Virus, lancée à l'aide de la commande KAVSHELL UPDATE, est une tâche temporaire. Elle apparaît dans la console de Kaspersky Anti-Virus dans MMC uniquement pendant son exécution. Le rapport sur l'exécution de la tâche est créé en même temps ; il apparaît dan le noeud Rapports de la console de Kaspersky Anti-Virus. A l'instar des tâches de mise à jour créées dans la console de Kaspersky Anti-Virus, les tâches de mise à jour créées et exécutées à l'aide de la commande KAVSHELL UPDATE seront soumises à la stratégie de Kaspersky Administration Kit (pour en savoir plus sur l'administration de Kaspersky Anti-Virus sur les serveurs à l'aide de Kaspersky Administration Kit, lisez le Partie 3 à la page 276).

Syntaxe de la commande KAVSHELL UPDATE

```
KAVSHELL UPDATE < Source de la mise à jour | /AK | /KL> [/NOUSEKL] [/PROXY:<adresse>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nom d'utilisateur>] [/PROXYPWD:<mot de passe>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE] [/TIMEOUT:<nombre de secondes>] [/REG:<код iso3166>] [/W:<nom du fichier de rappor>] [/ALIAS:<nom de tâche alternatif>]
```

Exemples de la commande KAVSHELL UPDATE

`KAVSHELL UPDATE` : lance la tâche de mise à jour des bases définie par l'utilisateur.

`KAVSHELL UPDATE \\Server\bases` : lance la mise à jour des bases, les fichiers des mises à jour se trouver dans le répertoire de réseau \\Server\bases.

`KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log` : lance la tâche de mise à jour depuis le serveur FTP ftp://dnl-ru1.kaspersky-labs.com/ ; consigne tous les événements de la tâche dans le fichier de rapport c:\update_report.log.

`KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456` : reçoit les mises à jour des bases de Kaspersky Anti-Virus du serveur des mises à jour de Kaspersky Lab ; établit la connexion via le serveur proxy (adresse du serveur proxy : proxy.company.com, port : 8080) ; l'accès au serveur requiert l'analyse intégrée de l'authenticité de Microsoft Windowd (authentification NTLM) sous le compte (nom d'utilisateur : inetuser, mot de passe : 123456).

Argument	Description
Sources de la mise à jour (argument obligatoire). Indiquez une ou plusieurs sources. Kaspersky Anti-Virus contactera chacune des sources dans l'ordre de la liste. Séparez les sources par un espace.	
<chemin au format UNC>	Source de mise à jour définie par l'utilisateur : chemin d'accès au répertoire de réseau contenant les mises à jour au format UNC (Universal Naming Convention). Vous pouvez utiliser des variables dans le chemin.
<URL>	Source des mises à jour définie par l'utilisateur : adresse du serveur FTP ou HTTP sur lequel se trouve le répertoire contenant les mises à jour.

Argument	Description
<Dossier local>	Source des mises à jour définie par l'utilisateur : répertoire sur le serveur protégé
/AK	Serveur d'administration de Kaspersky Administration Kit en guise de source des mises à jour
/KL	Serveurs de mises à jour de Kaspersky Lab en guise de source des mises à jour
/NOUSEKL	N'utilise pas les serveurs de mises à jour de Kaspersky Lab si les autres sources des mises à jour indiquées sont inaccessibles (utilisés par défaut)
Paramètres du serveur proxy	
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas cet argument, Kaspersky Anti-Virus identifiera automatiquement les paramètres du serveur proxy utilisé dans le répertoire local
/AUTHTYPE:<0-2>	Cet argument définit la méthode de vérification de l'authenticité pour l'accès au serveur proxy. Le paramètre peut prendre les valeurs suivantes : **0** : analyse de l'authenticité de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Anti-Virus contactera le serveur proxy sous le compte **Système local** (**SYSTEM**). **1** : analyse de l'authenticité de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Anti-Virus contactera le serveur proxy sous le compte utilisateur dont les données sont définies par les arguments /PROXYUSER et /PROXYPWD ; **2** : analyse de l'authenticité selon le nom et le mot de passe de l'utilisateur définis par les arguments /PROXYUSER et /PROXYPWD (Basic authentication). Si l'accès au serveur proxy ne requiert pas l'authentification, alors il n'est pas nécessaire d'indiquer cet argument.

Argument	Description
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur qui intervient pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> и /PROXYPWD:<mot de passe> sont ignorés
/PROXYPWD:<mot de passe>	Mot de passe qui intervient pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, alors les arguments /PROXYUSER:<nom d'utilisateur> и /PROXYPWD:<mot de passe> sont ignorés. Si vous définissez l'argument /PROXYUSER mais pas l'argument /PROXYPWD, alors le système considère que le mot de passe est vide
/NOPROXYFORKL	N'utilise pas les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab (utilisés par défaut)
/USEPROXYFORCUSTOM	Utilise les paramètres du serveur proxy pour la connexion aux sources de mises à jour définies par l'utilisateur (non utilisées par défaut)
/USEPROXYFORLOCAL	Utilise les paramètres du serveur proxy pour la connexion aux sources locales des mises à jour. Si cet argument n'est pas indiqué, la valeur **Ne pas utiliser les paramètres de proxy spécifiés pour se connecter aux sources des mises à jour locales** est appliquée. Pour obtenir de plus amples informations, sur ces paramètre, consultez le point B.5.4.1 à la page 426.
Paramètres généraux du serveur FTP ou HTTP	
/NOFTPPASSIVE	Si vous utilisez cet argument, Kaspersky Anti-Virus utilisera le mode actif du serveur FTP pour se connecter au serveur protégé. Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus utilisera le mode passif du serveur FTP si cela est possible.

Argument	Description
/TIMEOUT:<nombre de secondes>	Délai d'attente lors de la connexion au serveur FTP ou HTTP. Si vous n'utilisez pas cet argument, Kaspersky Anti-Virus appliquera la valeur par défaut : 10 s Cet argument accepte uniquement des nombres entiers.
/REG:<code iso3166>	L'argument des paramètres régionaux intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mises à jour le plus proche. En guise valeur pour cet argument, saisissez le code alphabétique du pays où se trouve le serveur protégé conformément à la norme ISO 3166-1, par exemple /REG:gr ou /REG:RU Si vous n'utilisez pas cet argument ou si vous indiquez un code inexistant, alors Kaspersky Anti-Virus identifiera l'emplacement du serveur protégé selon les paramètres régionaux du serveur protégé (pour Microsoft Windows 2003 Server ou suivant, il s'agit de la variable **Emplacement** (**Location**)).
/ALIAS:<nom alternatif de la tâche>	Cet argument permet d'attribuer un nom temporaire à la tâche afin de pouvoir la consulter durant l'exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à la l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants fonctionnels de Kaspersky Anti-Virus. Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_<kavshell_pid>, par exemple update_1234. Dans la console de Kaspersky Anti-Virus, la tâche reçoit le nom Updatebases (<date heure>), par exemple, Updatebases 8/16/2007 5:41:02 PM.

Argument	Description
/W:<nom du fichier du rapport>	Si vous désignez cet argument, Kaspersky Anti-Virus enregistre le fichier de rapport sur la tâche et lui donne le nom défini par l'argument. Le fichier du rapport contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le rapport reprend les événements définis par les paramètres des rapports et du journal des événements dans la console Kaspersky Anti-Virus (pour de plus amples informations, lisez le point 13.2.7 à la page 217). Vous pouvez indiquer un chemin absolu ou relatif au fichier du rapport. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier du rapport sera créé dans le répertoire en cours. Un nouveau lancement de la commande selon les mêmes paramètres de consignation écrase le fichier de rapport existant. Vous pouvez consulter le fichier du rapport durant l'exécution de la tâche d'analyse à la demande. Le rapport sur la tâche figure dans les nœuds **Rapports** de la console de Kaspersky Anti-Virus. Si Kaspersky Anti-Virus ne parvient pas à créer le fichier de rapport, il n'interrompt pas l'exécution de la commande et n'affiche pas de message sur l'erreur.

16.8. Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus. KAVSHELL ROLLBACK

La commande KAVSHELL ROLLBACK vous permet d'exécuter la tâche prédéfinie **Remise à l'état antérieur à la mise à jour** pour remettre les bases de Kaspersky Anti-Virus à l'état antérieur à la mise à jour. La commande est exécutée en mode synchrone.

Syntaxe de la commande

```
KAVSHELL ROLLBACK
```

16.9. Installation et suppression des clés. KAVSHELL LICENSE

La commande KAVSHELL LICENSE vous permet d'installer et de supprimer les clés de Kaspersky Anti-Virus.

Syntaxe de la commande KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD: <nom du fichier de clé> [/R] |
/DEL: <numéro de série>]
```

Exemples de la commande KAVSHELL LICENSE

`KAVSHELL LICENSE /ADD: C:/License.key` : installe un clé depuis le fichier ;

`KAVSHELL LICENSE` : récupère les informations sur les clés installées ;

`KAVSHELL LICENSE /DEL: 0000-000000-00000001` : supprime la clé installée avec le numéro de série 0000-000000-00000001.

Argument	Description
Sans argument	La commande affiche les informations suivantes sur les clés installées : • Numéro de série de la clé ; • Type de clé (test bêta, évaluation ou commerciale) ; • Durée de validité de la ; • La clé est-elle une clé de réserve. Si la valeur * est indiquée, alors la clé est installée en tant que clé de réserve.
/ADD: <nom du fichier de clé>	Installe la clé depuis un fichier dont le nom est défini par la valeur /ADD. Indiquez le nom du fichier de clé et le chemin d'accès complet à celle-ci.
/R	L'argument /R est complémentaire à l'argument /ADD. Il indique que la clé installée est une clé de réserve.
/DEL: <numéro de série>	Supprime la clé dont le numéro de série correspond à la valeur de l'argument /DEL.

16.10. Activation, configuration et désactivation de la constitution d'un journal de traçage. KAVSHELL TRACE

La commande KAVSHELL TRACE vous permet d'activer ou de désactiver sur-le-champ la création d'un journal de traçage de tous les sous-systèmes de Kaspersky Anti-Virus ainsi que de définir le niveau de détail des informations reprises dans le journal.

Syntaxe de la commande KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<dossier contenant les fichiers du journal de traçage> [/S:<taille maximale du fichier de traçage en mégaoctets>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Si le journal de traçage est constitué et que vous souhaitez modifier ses paramètres, alors saisissez la commande KAVSHELL TRACE avec l'argument /ON et définissez les paramètres du journal à l'aide des arguments /S et /LVL.

Argument	Description
/ON	Active la constitution du journal de traçage
/F:<dossier contenant les fichiers du journal de traçage>	Cet argument indique le chemin d'accès complet au dossier dans lequel les fichiers du journal de traçage seront conservés (argument obligatoire). Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Vous pouvez indiquer les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques de réseau du serveur protégé. Si le nom du dossier dont vous saisissez le chemin d'accès pour cet argument contient un espace, il faudra saisir le nom entre guillemets, par exemple /F:"C\Trace Folder".
/S:<Taille maximale du fichier journal en mégaoctets>	Cet argument définit la taille maximale d'un fichier du journal de traçage. Dès que la taille du journal atteint la valeur maximale, Kaspersky Anti-Virus consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé. Si vous ne définissez pas cet argument, la taille maximale d'un journal sera limitée à 50 Mo.
/LVL:<debug | info | warning | error | critical>	Cette clé définit le niveau de détail du journal depuis le niveau le plus détaillé (*informations de débogage*) où tous les événements sont enregistrés jusqu'au niveau minimum (*Critiques*) où seuls les événements critiques sont consignés dans le journal. Si vous ne définissez pas cet argument, alors le journal de traçage contiendra les événements correspondant au niveau de détail *Informaions de débogage*.
/OFF	Cet argument désactive la constitution du journal de traçage.

Exemples de commandes KAVSHELL TRACE :

`KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200` : active la constitution du journal de traçage au niveau de détail *`Informations de mise au`*

point avec une taille maximale de 200 Mo ; le journal sera enregistré dans le répertoire C:\Trace Folder.

`KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning` : active la constitution du journal de traçage au niveau de détail *Evénements importants* ; le journal sera enregistré dans le répertoire C:\Trace Folder.

`KAVSHELL TRACE /OFF` : désactive la constitution du journal de traçage.

16.11. Activation et désactivation de la création de fichiers de vidage. KAVSHELL DUMP

La commande KAVSHELL DUMP vous permet d'activer ou de désactiver sur le champ la création de modèles de mémoire (dumps) des processus de Kaspersky Anti-Virus en cas d'arrêt provoqué par une erreur. De plus, vous pouvez prendre à n'importe quel moment un exemple de la mémoire des processus de Kaspersky Anti-Virus en cours d'exécution.

Syntaxe de la commande KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<dossier contenant les fichiers de vidage>|/SNAPSHOT /F:<dossier contenant les fichiers de vidage> / P:<pid> | /OFF>
```

Exemples de commandes KAVSHELL DUMP :

`KAVSHELL DUMP /ON /F:"C:\Dump Folder"` : active la création d'un vidage ; enregistre les fichiers de vidage dans le répertoire C:\Dump Folder ;

`KAVSHELL DUMP /SNAPSHOT /F: C:/Dumps /P:1234` : capture le vidage de mémoire du processus avec l'identificateur 1234 dans le dossier C:/Dumps.

`KAVSHELL DUMP /OFF` : désactive la création du vidage.

Argument	Description
/ON	Active la création d'un vidage de mémoire du processus en cas d'arrêt suite à une erreur

Argument	Description
/F:<dossier contenant les fichiers de vidage>	Argument obligatoire ; indique le chemin d'accès au répertoire où le fichier de vidage sera enregistré. Si vous saisissez un chemin d'accès à un répertoire inexistant, le fichier ne sera pas créé. Vous pouvez indiquer les chemins de réseau au format UNC (Universal Naming Convention) mais vous ne pouvez pas indiquer les chemins d'accès aux répertoires sur les disques de réseau du serveur protégé.
/SNAPSHOT	Crée un instantané du modèle de mémoire du processus de Kaspersky Anti-Virus en exécution indiqué et enregistre le fichier de vidage dans le dossier dont le chemin d'accès est défini par l'argument /F.
/P	Identificateur du processus PID ; repris dans le gestionnaire des tâches de Microsoft Windows.
/OFF	Désactive la création d'un vidage de mémoire du processus en cas d'arrêt suite à une erreur.

16.12. Importations des paramètres. KAVSHELL IMPORT

La commande KAVSHELL IMPORT vous permet d'importer les paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches depuis un fichier de configuration dans Kaspersky Anti-Virus sur le serveur protégé. Vous pouvez créer le fichier de configuration à l'aide de la commande KAVSHELL EXPORT.

Syntaxe de la commande KAVSHELL IMPORT

```
KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de commandes KAVSHELL IMPORT

```
KAVSHELL IMPORT Server1.xml
```

Argument	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration d'où les paramètres vont être importés

16.13. Exportation des paramètres. KAVSHELL EXPORT

La commande KAVSHELL EXPORT vous permet d'exporter tous les paramètres de Kaspersky Anti-Virus et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Anti-Virus sur d'autres serveurs.

Syntaxe de la commande KAVSHELL EXPORT

```
KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples de commandes KAVSHELL EXPORT

```
KAVSHELL EXPORT Server1.xml
```

Argument	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration dans lequel les paramètres vont être enregistrés. Vous pouvez attribuer n'importe quelle extension au fichier de configuration.

CHAPITRE 17. CODE DE RETOUR

Les tableaux suivants décrivent les codes de retour des commandes de Kaspersky Anti-Virus.

Codes de retour des commandes KAVSHELL SCAN et KAVSHELL FULLSCAN

Code de retour	Description
0	L'opération a réussi (Aucune menace n'a été découverte).
1	L'opération a été annulée.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-4	L'objet est introuvable (le fichier avec la liste des couvertures d'analyse est introuvable).
-5	Syntaxe de la commande incorrect ou couverture d'analyse non définie.
-80	Des objets infectés ont été découverts.
-81	Des objets suspects ont été découverts.

Codes de retour des commandes KAVSHELL START et KAVSHELL STOP

Code de retour	Description
-82	Des erreurs de fonctionnement ont été découvertes.
-83	Des objets non vérifiés ont été découverts.
-84	Des objets corrompus ont été découverts.
-6	Opération invalide (par exemple, le service de Kaspersky Anti-Virus est déjà exécuté ou est déjà arrêté).
-7	Le service n'est pas enregistré.
-8	Le lancement du service est interdit.

Code de retour	Description
-9	La tentative d'exécution du service sous un autre compte utilisateur a échoué (par défaut, le service de Kaspersky Anti-Virus fonctionne sous compte utilisateur **Système local**).
-99	Erreur inconnue.

Codes de retour de la commande KAVSHELL TASK

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-4	L'objet est introuvable (la tâche est introuvable).
-5	Syntaxe de la commande incorrecte.
-6	Opération invalide (par exemple, la tâche n'est pas lancée, est déjà lancée ou ne peut être arrêtée).
-99	Erreur inconnue.
-301	Clé invalide.
401	La tâche n'est pas lancée (pour l'argument /STATE).
402	La tâche est déjà lancée (pour l'argument /STATE).
403	La tâche est déjà arrêtée (pour l'argument /STATE).
-404	Erreur d'exécution de l'opération (la modification de l'état de la tâche a entraîné son échec).

Codes de retour de la commande KAVSHELL LICENSE

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Privilèges insuffisants pour l'administration des clés.

Code de retour	Description
-4	Objet introuvable (la clé portant ce numéro de série est introuvable).
-5	Syntaxe de la commande incorrecte.
-6	Opération invalide (la clé est déjà installée).
-99	Erreur inconnue.
-301	Clé invalide.
-303	La clé est prévue pour une autre application.

Codes de retour de la commande KAVSHELL UPDATE

Code de retour	Description
0	L'opération a réussi.
200	Tous les objets sont d'actualité (les bases ou les modules logiciels sont d'actualité).
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-5	Syntaxe de la commande incorrecte.
-99	Erreur inconnue.
-206	Les fichiers des mises à jour ne sont pas présents dans la source indiquée ou leur format est inconnu.
-209	Erreur de connexion à la source des mises a jour.
-232	Kaspersky Anti-Virus n'a pas réussi la vérification de l'authenticité lors de la connexion au serveur proxy.
-234	Erreur de connexion à l'application Kaspersky Administration Kit.
-235	Kaspersky Anti-Virus n'a pas réussi la vérification de l'authenticité lors de la connexion à la source des mises à jour.
-301	Clé invalide.

Codes de retour de la commande KAVSHELL ROLLBACK

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-99	Erreur inconnue.
-221	La copie de sauvegarde des bases est introuvable.
-222	La copie de sauvegarde des bases est corrompue.

Codes de retour de la commande KAVSHELL RTP

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-4	L'objet est introuvable (une des tâches de protection en temps réel ou toutes les tâches de protection en temps réel sont introuvables).
-5	Syntaxe de la commande incorrecte.
-6	Opération invalide (par exemple, la tâche est déjà exécutée ou est déjà arrêtée).
-99	Erreur inconnue.
-301	Clé invalide.

Codes de retour de la commande KAVSHELL DUMP

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.

Code de retour	Description
-4	L'objet est introuvable (le chemin indiqué en guise de chemin d'accès au dossier contenant les fichiers de vidage est introuvable ; le processus avec le PID indiqué est introuvable).
-5	Syntaxe de la commande incorrecte.
-6	Opération invalide (l'attempte d'execution de KAVSHELL DUMP /OFF si la création des fichiers de vidage est déjà désactivée).
-99	Erreur inconnue.

Codes de retour de la commande KAVSHELL TRACE

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-4	L'objet est introuvable (le chemin d'accès indiqué en tant que chemin d'accès au dossier contenant les fichiers du journal de traçage est introuvable).
-5	Syntaxe de la commande incorrecte.
-6	Opération invalide (la création du journal de traçage est déjà activée ou désactivée).
-99	Erreur inconnue.

Codes de retour de la commande KAVSHELL IMPORT

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-4	L'objet est introuvable (le fichier de configuration à importer est introuvable).

Code de retour	Description
-5	Syntaxe incorrecte.
-99	Erreur inconnue.
-501	L'opération a réussi ; toutefois durant l'exécution de la commande, une erreur / une remarque est apparue, par exemple Kaspersky Anti-Virus n'a pas exporté les paramètres d'un des composants.
-502	Le format du fichier à importer est inconnu ou le fichier manque.
-503	Paramètres incompatibles (le fichier de configuration provient d'une autre application ou d'une version de Kaspersky Anti-Virus postérieure ou incompatible).

Codes de retour de la commande KAVSHELL EXPORT

Code de retour	Description
0	L'opération a réussi.
-2	Le service n'est pas lancé.
-3	Erreur de privilèges d'accès.
-5	Syntaxe incorrecte.
-10	Impossible de créer le fichier de configuration (par exemple, accès interdit au répertoire indiqué dans le chemin d'accès au fichier).
-99	Erreur inconnue.
501	L'opération a réussi ; toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple Kaspersky Anti-Virus n'a pas exporté des paramètres d'un composant fonctionnel quelconque.

PARTIE 3. CONFIGURATION DE L'ADMINISTRATION VIA KASPERSKY ADMINISTRATION KIT

Si votre entreprise a adopté Kaspersky Administration Kit pour l'administration centralisée des logiciels antivirus, vous pouvez utiliser la console d'administration de Kaspersky Administration Kit pour administrer et configurer Kaspersky Anti-Virus sur les serveurs protégés.

Cette section aborde les sujets suivants :

- Administration de Kaspersky Anti-Virus et consultation de son état (cf. Chapitre 18, p. 277) ;
- Création et configuration des stratégies (cf. Chapitre 19, p. 287) ;
- Configuration de Kaspersky Anti-Virus dans la boîte de dialogue **Paramètres de l'application** cf. Chapitre 20 p. 301) ;
- Création et configuration des tâches (cf. Chapitre 21, p. 334).

CHAPITRE 18. ADMINISTRATION DE KASPERSKY ANTI-VIRUS ET CONSULTATION DE SON ETAT

Le présent chapitre aborde les informations suivantes :

- Lancement et arrêt du service de Kaspersky Anti-Virus (cf. point 18.1, p. 277) ;
- Consultation de l'état de protection du serveur (cf. point 18.2, p. 278) ;
- Consultation des statistiques de Kaspersky Anti-Virus (cf. point 18.3, p. 281) ;
- Consultation des informations relatives à Kaspersky Anti-Virus (cf. point 18.4, p. 283) ;
- Consultation des informations relatives aux clés installées (cf. point 18.5, p. 284).

18.1. Lancement et arrêt du service de Kaspersky Anti-Virus

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

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

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

Afin de lancer ou d'arrêter le service de Kaspersky Anti-Virus :

1. Dans l'arborescence de la console d'administration, déployez l'entrée **Groupes** et sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel sur la ligne contenant les informations relatives au serveur protégé et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés: <nom de l'ordinateur>** sous l'onglet **Applications**, sélectionnez la commande **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** dans la liste des applications installées puis cliquez sur le bouton **Propriétés**.
4. Dans la boîte de dialogue **Paramètres de l'application**, ouvrez l'onglet **Général**.
5. Exécutez une des actions suivantes :
   - Pour lancer le service de Kaspersky Anti-Virus, cliquez sur le bouton **Démarrer** ;
   - Pour arrêter le service de Kaspersky Anti-Virus, cliquez sur le bouton **Stopper**.
6. Cliquez sur **OK**.

18.2. Consultation de l'état de la protection du serveur

La console d'administration vous permet de consulter l'état de la protection du serveur sélectionné : état des tâches **Protection en temps réel des fichiers** et **Analyse des scripts**, état général de la sécurité antivirus et de l'accessibilité du serveur.

Pour consulter l'état de la protection du serveur sélectionné :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : <nom de l'ordinateur>** , ouvrez le paramètre **Protection** (cf. ill. 93).

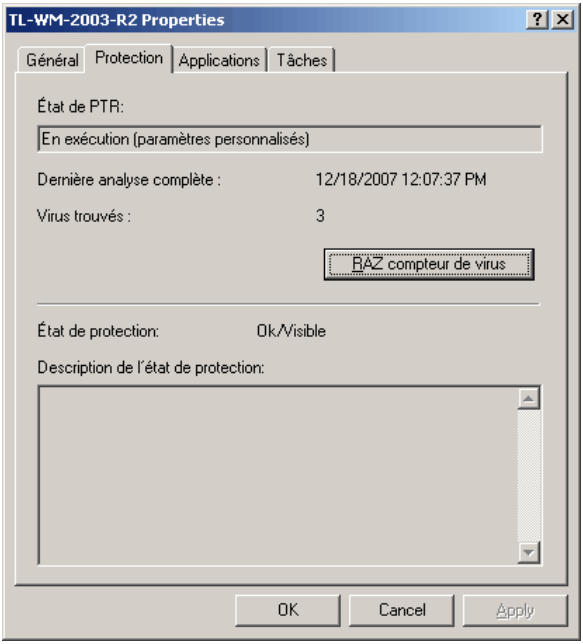

Illustration 93. Boîte de dialogue **Propriétés : <nom de l'ordinateur>,** onglet **Protection**

L'onglet **Protection** reprend les informations suivantes au sujet du serveur protégé :

Tableau 23. Information au sujet du serveur protégé sur l'onglet **Protection**

Champ	Description
Etat de PTR	Affiche l'état de la protection en temps réel : **En exécution**, si la tâche **Protection en temps réel des fichiers** ou la tâche **Analyse des scripts** est en cours. Si la tâche **Protection en temps réel des fichiers** est en cours, l'état de la protection en temps réel indique le nom du niveau de protection appliqué à la tâche : • **Recommandé**. Les paramètres de la protection correspondent à ceux du niveau **Recommandé** ; • **Protection maximale**. Les paramètres de la protection correspondent à ceux du niveau **Protection maximale** ; • **Vitesse maximale**. Les paramètres de la protection correspondent à ceux du niveau **Vitesse maximale** ; • **Paramètres utilisateur**. Les paramètres de la protection définis pour la tâche correspondent à ceux du niveau **Personnalisée**. Pour obtenir de plus amples informations sur les niveaux de protection offerts, lisez le point 6.2.2.1 à la page 79.
Dernière analyse complète	Date et heure de la dernière exécution de l'analyse à la demande qui a l'état « tâche d'analyse complète de l'ordinateur ».
Virus trouvès	Nombre total de programmes malveillants (noms des menaces) découverts sur le serveur protégé (compteur des menaces identifiées) depuis la dernière installation de Kaspersky Anti-Virus ou depuis la remise à zéro du compteur. Pour remettre le compte à zéro, cliquez sur le bouton **RAZ compteur des virus**.
Etat de protection	Etat du serveur du point de vue de la sécurité contre les virus. Pour en savoir plus sur les états de l'ordinateur, lisez le site du service d'assistance technique de Kaspersky Lab, code de l'article : **987**.

18.3. Consultation des statistiques de Kaspersky Anti-Virus

La console d'administration vous permet de consulter les statistiques de Kaspersky Anti-Virus sur le serveur protégé sélectionné : nombre de processus de Kaspersky Anti-Virus exécutés, nombre de signatures dans les bases de Kaspersky Anti-Virus installées sur le serveur, date de création des dernières mises à jour des bases installées et renseignements sur le fonctionnement de divers composants de Kaspersky Anti-Virus et sur l'exécution des tâches.

Remarque

Si vous souhaitez consulter les statistiques de Kaspersky Anti-Virus en temps réel, ouvrez le port UDP 15000 du pare-feu Windows de l'ordinateur sur lequel la serveur d'administration est affichée.

Pour consulter les statistiques de Kaspersky Anti-Virus :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres de l'ordinateur (propriétés)**, sur l'onglet **Applications**, sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** les applications antivirus installées dans la liste puis, cliquez sur **Statistiques**. La boîte de dialogue **Statistiques** s'ouvre (cf. ill. 94).

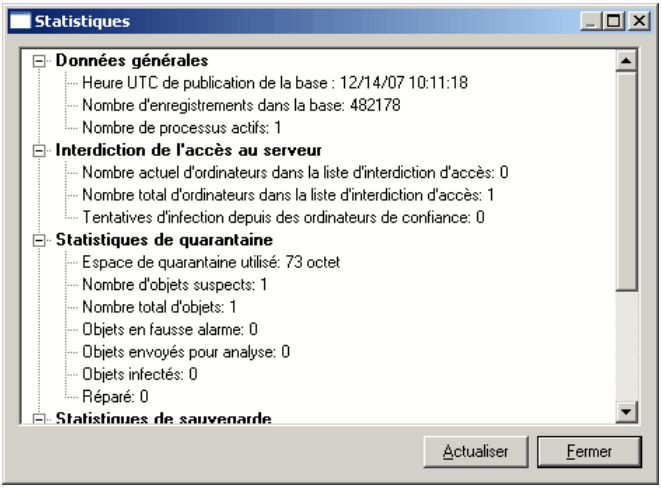

Illustration 94. Boîte de dialogue **Statistiques**

La boîte de dialogue **Statistiques** contient les informations suivantes :

Tableau 24. Information sur l'état d'Anti-Virus sur la serveur protégée

Champ	Description
Heure UTC de création de la base	Date et heure de création par Kaspersky Lab des dernières bases de l'application installées. L'heure est exprimée en temps universel (TU).
Nombre de processus de travail actifs	Nombre de processus de Kaspersky Anti-Virus dans lesquels les tâches de la protection en temps réel, de l'analyse à la demande et de la mise à jour sont en cours d'exécution.
Nombre d'enregistrements dans la base	Nombre total d'enregistrements dans les bases de Kaspersky Anti-Virus installées sur le serveur.
Statistiques de quarantaine	Renseignements sur l'état actuel de la quarantaine (pour en savoir plus, consultez le point 11.9 à la page 188).
Statistiques de la protection en temps réel des fichiers	Renseignements sur l'état actuel de la **Protection en temps réel des fichiers** (pour en savoir plus, consultez le point 6.2.3 à la page 91).

Champ	Description
Statistiques de l'interdiction	Informations sur le nombre d'ordinateurs dont l'accès au serveur protégé a été interdit depuis la dernière exécution de Kaspersky Anti-Virus (pour de plus amples informations, lisez le point 7.9, p. 107).
Statistiques de l'analyse à la demande	Renseignements sur les tâches d'analyse à la demande en cours d'exécution (pour en savoir plus, consultez le point 9.4 à la page 147).
Statistiques de surveillance des scripts	Renseignements sur le nombre de scripts traités par Kaspersky Anti-Virus depuis le lancement de la tâche **Analyse des scripts** jusqu'à maintenant (pour en savoir plus, consultez le point 6.5, p. 95).
Statistiques de sauvegarde	Renseignements sur l'état actuel de la sauvegarde (pour en savoir plus, consultez le point 12.6 à la page 202).

Remarque

Les informations relatives aux tâches **Protection en temps réel des fichiers** et **Analyse des scripts** ainsi qu'aux tâches d'analyse à la demande sont affichées uniquement lors que la tâche correspondante est en cours d'exécution.

18.4. Consultation des informations relatives à Kaspersky Anti-Virus

Vous pouvez consulter les informations relatives à Kaspersky Anti-Virus et à ses bases.

Pour afficher les informations relatives à Kaspersky Anti-Virus :

1. Dans l'arborescence de la console d'administration, déployez l'entrée **Groupes** et sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel sur la ligne contenant les informations relatives au serveur protégé et sélectionnez la commande **Propriétés**.

3. Dans la boîte de dialogue **Propriétés: <nom de l'ordinateur>** sous l'onglet **Applications**, sélectionnez la commande **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** dans la liste des applications installées puis cliquez sur le bouton **Propriétés**.
4. Dans la boîte de dialogue **Paramètres de l'application**, ouvrez l'onglet **Général**.

L'onglet **Général** (cf. ill. 103) fournit les informations suivantes :

- Renseignements généraux sur Kaspersky Anti-Virus :
  - Numéro de la version ;
  - Date et heure de l'installation ;
  - Date et heure de la dernière mise à jour des modules de Kaspersky Anti-Virus ;
  - Etat du service de Kaspersky Anti-Virus (exécuté / arrêté).
- Renseignements sur les bases antivirus :
  - Date et heure de création des bases des mises à jour installées (au format correspondant à la configuration régionale de l'ordinateur où est installée la console d'administration) ;
  - Nombre total d'enregistrements dans les bases ;
  - Date et l'heure de la dernière mise à jour.

18.5. Consultation des informations relatives aux clés installées

Pour consulter les informations relatives aux clés installées,

1. Dans l'arborescence de la console d'administration, déployez l'entrée **Groupes** et sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel sur la ligne contenant les informations relatives au serveur protégé et sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés: <nom de l'ordinateur>** sous l'onglet **Applications**, sélectionnez la commande **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** dans la liste des applications installées puis cliquez sur le bouton **Propriétés**.

4. Dans la boîte de dialogue **Paramètres de l'application**, ouvrez l'onglet **Licence** (cf. ill. 95).

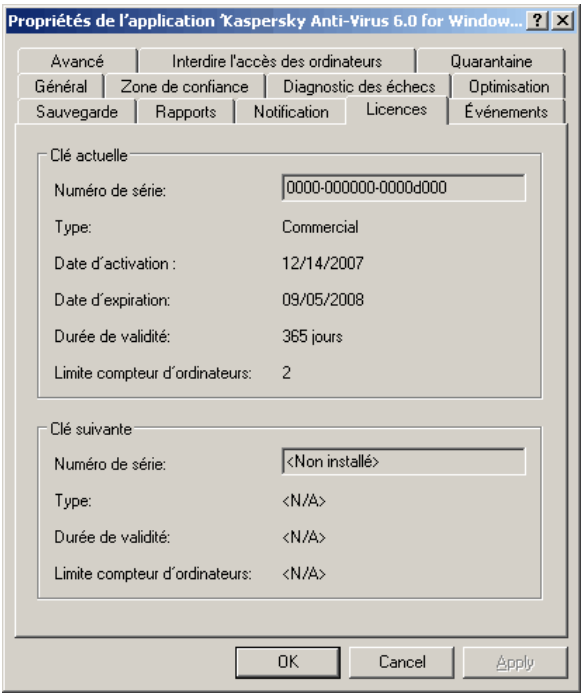

Illustration 95. Boîte de dialogue **Propriètès de l'application**, onglet **Licences**

L'onglet **Licences** propose les informations suivantes relatives aux clés installées :

Tableau 25. Information sur les clés installées

Champ	Description
Numéro de série	Numéro de série de la clé
Type	Type de clé (test bêta, clé d'évaluation ou clé commerciale). Pour en savoir plus sur les types de clé, consultez le point 14.1, p 230.
Date d'activation	Date d'installation de la clé (uniquement pour la clé active)

Champ	Description
Date d'expiration	Date de fin de validité de la clé (uniquement pour la clé active) ; déterminée par Kaspersky Anti-Virus lors de l'installation de la clé ; correspond à la fin de la *période de validité de la clé* depuis son activation mais elle ne peut être ultérieure à la *date à laquelle la clé n'est plus valide*
Durée de validité	Nombre de jours avant l'expiration de la licence
Limite compteur d'ordinateurs	Restriction prévue par la clé (le cas échéant)

CHAPITRE 19. CREATION ET CONFIGURATION DE STRATEGIE

Le présent chapitre aborde les sujets suivants :

- Présentation des stratégies (cf. point 19.1, p. 287) ;
- Création de stratégie (cf. point 19.2, p. 288) ;
- Configuration d'une stratégie (cf. point 19.3, p. 294) ;
- Désactivation du lancement programmé des tâches prédéfinies locales (cf. point 19.4, p. 299).

19.1. Présentation des stratégies

Vous pouvez créer des stratégies de Kaspersky Administration Kit unique pour l'administration de la protection de plusieurs serveurs sur lesquels Kaspersky Anti-Virus est installé.

Une *stratégie* applique les paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches à l'ensemble des serveurs protégés au sein d'un groupe d'administration.

Remarque

Les stratégies ne vous permettent pas de constituer une couverture de protection (analyse) dans les tâches **Protection en temps réel des fichiers** ni dans les tâches d'analyse à la demande.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la console, la stratégie d'administration active dans le groupe en ce moment possède l'état *active*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Anti-Virus. Vous pouvez la consulter dans la console de Kaspersky Anti-Virus dans MMC dans le noeud **Enregistrement d'audit système**.

Parmi toutes les méthodes d'application des stratégies, vous pouvez utiliser uniquement la méthode **Ne pas modifier les paramètres** qui ne prévoit pas l'enre-

gistrement des valeurs des paramètres définis par la stratégie dans Kaspersky Anti-Virus. Vous ne pouvez pas utiliser les méthodes d'application des stratégies **Modifier les paramètres obligatoires** et **Modifier tous les paramètres**.

Conformément à la méthode d'application de la stratégie **Ne pas modifier les paramètres**, Kaspersky Anti-Virus applique les valeurs des paramètres en regard desquels vous avez coché la case 🔒 dans les propriétés de la stratégie au lieu de la valeur des paramètres effectifs avant l'application de la stratégie. Les paramètres accompagnés de l'icône 🔓 dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Anti-Virus. Dès que la stratégie n'est plus appliquée, les paramètres dont les valeurs étaient modifiées par la stratégie retrouvent les valeurs qu'ils avaient avant l'application de la stratégie.

Tandis que la stratégie est appliquée, la console de Kaspersky Anti-Virus dans MMC et la boîte de dialogue **Propriétés de l'application** de la console d'administration affichent les valeurs des paramètres marqués dans la stratégie par l'icône 🔒 ; ils ne peuvent être modifiés. Les valeurs des autres paramètres (indiqués dans la stratégie par l'icône 🔓) peuvent être modifiés dans la console de Kaspersky Anti-Virus dans MMC et dans la boîte de dialogue **Propriétés de l'application** de la console d'administration.

Si la stratégie définit les paramètres d'une tâche quelconque de protection en temps réel et que celle-ci est exécutée, alors ces paramètres définis par la stratégies sont appliqués immédiatement dès que la stratégie devient active. Si la tâche n'est pas exécutée, alors les paramètres sont appliqués à son lancement. Si la stratégie définit les paramètres d'autres tâches de Kaspersky Anti-Virus, alors quand la stratégie devient active, ces paramètres ne sont pas appliqué aux tâches en cours d'exécution mais uniquement lors du prochain lancement de la tâche.

19.2. Création d'une stratégie

La création d'une nouvelle stratégie comprend deux étapes :

5. Vous pouvez créer une stratégie à l'aide de l'Assistant de création de stratégie. Les différentes fenêtres de l'Assistant vous permettent de définir les paramètres des tâches **Mise à jour des bases**, **Mise à jour des modules de l'application**, **Protection en temps réel des fichiers** et **Analyse à la demande**.

6. La boîte de dialogue **Paramètres de la stratégie** vous permet de définir les paramètres des tâches et les paramètres de Kaspersky Anti-Virus en fonction de vos besoins.

   La boîte de dialogue **Paramètres de la stratégie** vous permet de modifier les paramètres de mise à jour, d'analyse à la demande et de **protection en temps réel des fichiers** définis à l'aide de l'Assistant de

création de stratégie. Pour en savoir plus sur la manière de procéder à la création d'une tâche, consultez le point 19.3 à la page 294.

Pour créer une stratégie pour un groupe de serveurs sur lesquels Kaspersky Anti-Virus est installé :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis ouvrez le groupe d'administration pour les serveurs auxquels la stratégie sera appliquée.
2. Dans le menu contextuel du sous-noeud **Stratégies**, sélectionnez la commande **Nouvelle** → **Stratégie**.

   La fenêtre de l'Assistant de création de stratégies s'ouvre.
3. Dans la fenêtre **Nom de la stratégie**, saisissez le nom de la stratégie créée dans le champ prévu à cet effet. (Le nom ne peut contenir les symboles **" * < : > ? \ / |**).
4. Sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** dans la fenêtre **Applications** sous le titre **Application**.
5. Sélectionnez un des états de stratégie suivant dans la fenêtre **Nouvelle stratégie** :

   - **Active**, si vous souhaitez que la stratégie entre en vigueur dès après sa création. Si le groupe contient déjà une stratégie active, celle-ci deviendra inactive et la stratégie que vous venez de créer sera activée.
   - **Inactive** si vous ne souhaitez pas appliquer la stratégie créée. Vous pouvez activer la stratégie plus tard.

   Les fenêtres suivantes de l'Assistant de création de stratégie vous permettent de définir les paramètres des tâches **Mise à jour des bases**, **Mise à jour des modules de l'application**, **Protection en temps réel des fichiers** et **Analyse à la demande** en fonction de vos besoins.
6. Dans la fenêtre **Protection en temps réel des fichiers** (cf. ill. 96), sélectionnez le mode de protection des objets dans la tâche **Protection en temps réel des fichiers** et sélectionnez un des niveaux de sécurité proposé ou configurez les paramètres de la protection (cf. point B.3 à la page 398).

   Cochez la case **Appliquer la zone de confiance** si, dans la tâche **Protection en temps réel des fichiers**, vous souhaitez exclure de l'analyse les objets décrits dans la zone de confiance de Kaspersky Anti-Virus (pour de plus amples informations sur la zone de confiance, lisez le point 8.1 à la page 109 ; pour savoir comment ajouter des exclusions à la zone de confiance dans Kaspersky Administration Kit, lisez le point 20.7 à la page 325).

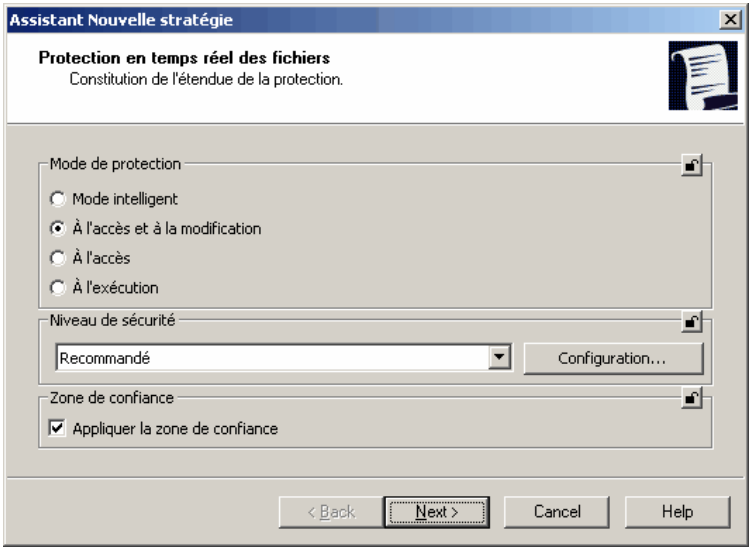

Illustration 96. Fenêtre **Protection en temps réel des fichiers**

1. Dans la fenêtre **Analyse à la demande** (cf. ill. 97), sélectionnez un des niveaux de sécurité prédéfinis ou configurez manuellement les paramètres de sécurité dans les tâches d'analyse à la demande (B.3 à la page 398).

   Cochez la case Appliquer la zone de confiance si, dans la tâche Protection en temps réel des fichiers, vous souhaitez exclure de l'analyse les objets décrits dans la zone de confiance de Kaspersky Anti-Virus (pour de plus amples informations sur la zone de confiance, lisez le point 8.1 à la page 109 ; pour savoir comment ajouter des exclusions à la zone de confiance dans Kaspersky Administration Kit, lisez le point 20.7 à la page 325).

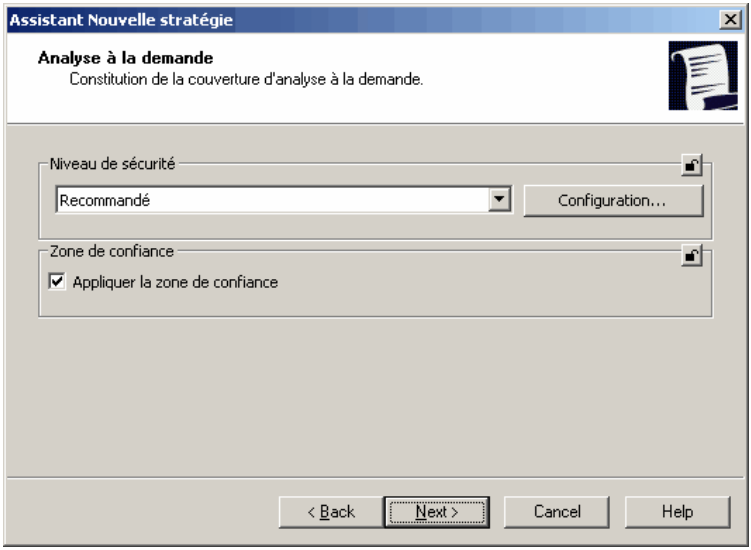

Illustration 97. Fenêtre **Analyse à la demande**

2. Dans la fenêtre **Mettre à jour** (cf. ill. 98), configurez les paramètres des tâches **Mise à jour de la base de données de l'application** et **Mise à jour des modules de l'application**.
3. Exécutez les actions suivantes dans la fenêtre **Paramètres** :
   a) Sélectionnez la source des mises à jour (cf. point B.5.1, p. 423) ;

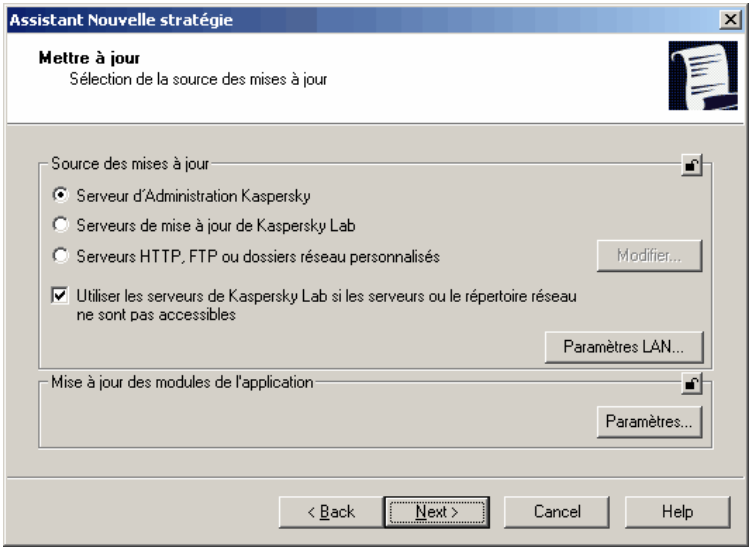

Illustration 98. Fenêtre **Mettre à jour**

b) Cliquez sur le bouton **Paramètres LAN**. Configurez les paramètres requis dans la boîte de dialogue **Paramètres de connexion** :

- Modifiez le mode du serveur FTP pour la connexion au serveur protégé et le délai d'attente de connexion (cf. point B.5.2, p. 424) ;
- Configurez les paramètres d'accès au serveur proxy pour la connexion à la source des mises à jour (cf. point B.5.4, p. 425) ;
- Sur l'onglet **Paramètres régionaux**, précisez l'emplacement du(des) serveur(s) protégé(s) afin d'optimaliser la réception des mises à jour (cf. point B.5.5, p. 429).

c) Pour configurer les paramètres de la tâche de **Mise à jour des modules de l'application**, cliquez sur le bouton **Paramètres** dans la fenêtre **Mise à jour** sous le titre **Mise à jour des modules de l'application** et configurez les paramètres de la mise à jour des modules de l'application dans la boîte de dialogue **Paramètres de mise à jour des modules de produits** (cf. ill. 99).

- Décidez si vous souhaitez charger et installer la mise à jour des modules de l'application ou uniquement vérifier si elles sont disponibles. (cf. point B.5.6.1, p. 431).

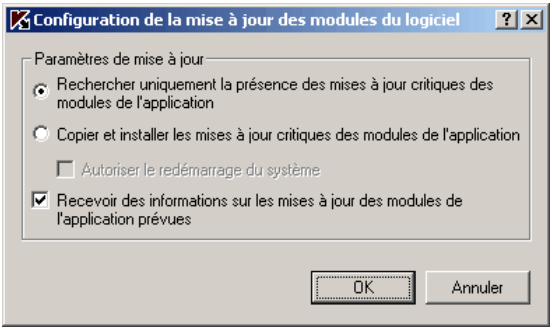

Illustration 99. Boîte de dialogue **Configuration de la mise à jour des modules du logiciel**

- Pour qu'à la fin de la tâche Kaspersky Anti-Virus redémarre automatiquement le serveur si cette opération s'impose pour l'application des modules logiciels installés, cochez la case **Autoriser le redémarrage du système**.
- Si vous souhaitez obtenir des informations sur la diffusion des mises à jour prévues des modules de l'application, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

  Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez configurer les notifications adressées à l'administrateur pour l'événement **Une mise à jour prévue des modules de Kaspersky Anti-Virus sont disponibles**. Cette notification reprend l'adresse des pages de notre site d'où la mise à jour prévue pourra être téléchargée (pour de plus amples informations sur la configuration des notifications, consultez le point 15.2 à la page 238).

> **Remarque**
>
> Les paramètres de la tâche **Copie des mises à jour** peuvent être configurés ultérieurement dans la boîte de dialogue **Paramètres de la stratégie**.

4. Dans la fenêtre **Fin du travail**, cliquez sur le bouton **Terminer**.

La stratégie créée est reprise dans la liste des stratégies du noeud **Stratégies** du groupe d'administration sélectionné. Dans la boîte de dialogue **Paramètres de la stratégie**, vous pouvez configurer d'autres paramètres de Kaspersky Anti-Virus, de ses fonctions et de ses tâches.

19.3. Configuration des stratégies

Dans la boîte de dialogue **Propriétés** de la stratégie existante, vous pouvez configurer les paramètres généraux de Kaspersky Anti-Virus, les paramètres de ses fonctions et de ses tâches pour les serveurs.

Remarque

La stratégie ne vous permet de constituer une couverture de protection (analyse) dans la tâche **Protection en temps réel des fichiers** ni dans les tâches d'analyse à la demande.

*Pour configurer les paramètres dans la boîte de dialogue **Paramètres de la stratégie** :*

1. Dans l'arborescence de la console d'administration, déployez le nœud **Groupe** puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie puis déployez le nœud **Stratégie**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la stratégie contenant les paramètres que vous souhaitez modifier puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : <nom de la stratégie>** (cf. ill. 100), configurez les paramètres requis de la stratégie.

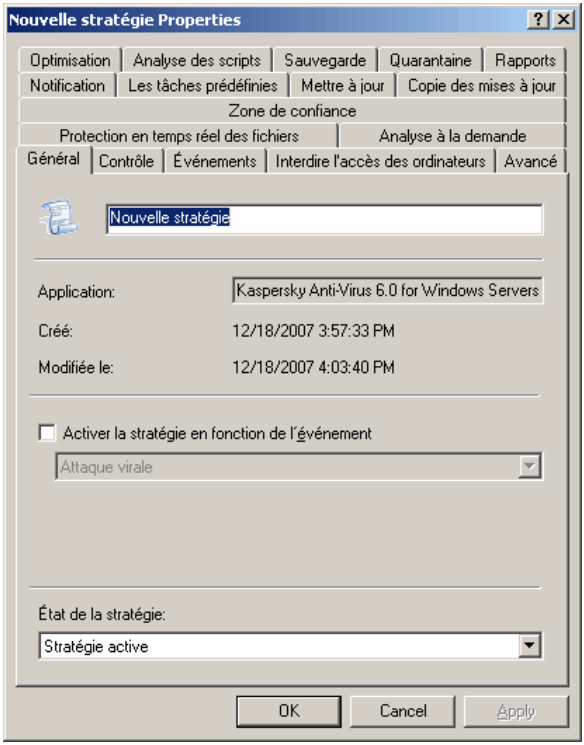

Illustration 100. Exemple de boîte de dialogue **Paramètres : <nom de la stratégie>**

Vous pouvez configurer les paramètres de la stratégie sur les onglets suivants :

Tableau 26. Configuration des paramètres de la stratégie

Paramètres	Onglet
Paramètres de protection dans la tâche **Protection en temps réel des fichiers** : • **Mode de protection des objets** (cf. description du paramètre au point B.3.1, p. 399) ; • **Paramètre de protection** (uniques pour toutes les couvertures d'analyse) : vous pouvez sélectionner un niveau de protection prédéfini (cf. description au point 6.2.2.1, p. 79) ou configurer manuellement les paramètres de sécurité (comme dans la console MMC, cf. les instructions à la page 82).	**Protection en temps réel des fichiers**
• Paramètres d'interdiction automatique de l'accès des ordinateurs (cf. instructions à la page 310) ; • exclusion des ordinateurs de l'interdiction (ordinateurs de confiance) (cf. les instructions à la page 311) ; • prévention des épidémies virales (cf. les instructions à la page 312).	**Interdire l'accès des ordinateurs**
• Autorisation ou interdiction de l'exécution des scripts suspects (pour en savoir plus sur ce paramètre, lisez le point 6.1 à la page 68) ; Application de la zone de confiance (pour en savoir plus sur la zone de confiance, consultez le Chapitre 8 à la page 109).	**Analyse des scripts**

Paramètres	Onglet
• Administration de la liste des processus de confiance (comme dans la boîte de dialogue **Paramètres de l'application**, cf. point 20.7.1, p. 325). • Désactivation de la protection en temps réel des fichiers sollicités pendant les opérations de sauvegarde (comme dans la boîte de dialogue **Paramètres de l'application**, cf. point 20.7.2 à la page 327. • Création et application des exclusions de la zone de confiance (cf. point 20.7, p. 325).	**Zone de confiance**
Paramètres de sécurité dans la tâche d'analyse à la demande (uniques pour toute la couverture d'analyse): vous pouvez sélectionner un niveau de protection prédéfini (cf. description au point 9.2.2.1, p. 132) ou configurer manuellement les paramètres de sécurité (comme dans la console MMC, cf. les instructions à la page 137).	**Analyse à la demande**
Paramètres des tâches de mise à jour **Mise à jour des bases** et **Mise à jour de l'application** : • Sélectionner la source des mises à jour (pour obtenir de plus amples informations sur le paramètre, lisez le point B.5.1 à la page 423) ; • configurer les paramètres de connexion à la source des mises à jour et indiquez l'emplacement du serveur protégé pour optimiser les mises à jour (boutons **Configuration LAN**) (comme dans la console MMC, cf. les instructions à la page 162) ; • configurer les paramètres de la tâche **Mise à jour des modules de l'application** (bouton **Configuration**) (comme dans la console MMC, cf. les instructions à la page 165).	**Mettre à jour**

Paramètres	Onglet
Paramètres de la tâche **Copie des mises à jour** : • sélectionner la source des mises à jour (pour obtenir de plus amples informations sur le paramètre, lisez le point B.5.1 à la page 423) ; • configurer les paramètres de connexion à la source des mises à jour et indiquez l'emplacement du serveur protégé pour optimiser les mises à jour (boutons **Configuration LAN**) (comme dans la console MMC, cf. les instructions à la page 162) ; • configurer les paramètres de la tâche **Copie des mises à jour** (comme dans la console MMC, cf. les instructions à la page 167).	**Copie des mises à jour**
Désactivation de l'action de la programmation des tâches système (cf. point 19.4, p. 299)	**Les tâches prédéfinies**
Paramètres de quarantaine (comme dans la boîte de dialogue **Paramètres de l'application**, cf. l'instruction à la page 318)	**Quarantaine**
Paramètres de sauvegarde (comme dans la boîte de dialogue **Paramètres de l'application**, cf. l'instruction à la page 321)	**Sauvegarde**
Paramètres généraux de Kaspersky Anti-Virus	**Avancé**
Configuration des notifications relatives aux événements de Kaspersky Anti-Virus envoyées à l'administrateur et aux utilisateurs	**Notification**
Configuration des rapports	**Rapports**
Configuration des notifications relatives aux événements de Kaspersky Anti-Virus envoyées à l'administrateur et aux utilisateurs	**Événements**

4. Une fois que vous aurez modifié les différents paramètres de la stratégie, cliquez sur le bouton **OK** pour enregistrer les modifications.

19.4. Désactivation / rétablissement du lancement programmé des tâches prédéfinies locales

Grâce aux stratégies, vous pouvez désactiver l'exécution programmée des tâches prédéfinies locales suivantes sur l'ensemble des serveurs d'un groupe d'administration :

- Tâches **Protection en temps réel des fichiers** ;
- Tâches **Analyse des scripts** ;
- Tâche d'analyse à la demande **Analyse de l'ordinateur**, **Analyse des objets en quarantaine, Analyse au démarrage du système** et **Analyse de l'intégrité de l'application** ;
- Les tâches de mise à jour **Mise à jour des bases de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**.

Remarque

Si vous excluez le serveur protégé du groupe d'administration, la planification des tâches prédéfinies sera automatiquement activée.

Pour désactiver le lancement programmé d'une tâche prédéfinie de Kaspersky Anti-Virus sur les serveurs du groupe :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes**, déployez ensuite le groupe requis puis, sélectionnez le noeud **Stratégies**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la stratégie à l'aide de laquelle vous souhaitez désactiver le lancement programmé des tâches prédéfinies de Kaspersky Anti-Virus sur les serveur du groupe et sélectionnez le point **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : <nom de la stratégie>**, ouvrez l'onglet **Les tâches prédéfinies** (cf. ill. 101).

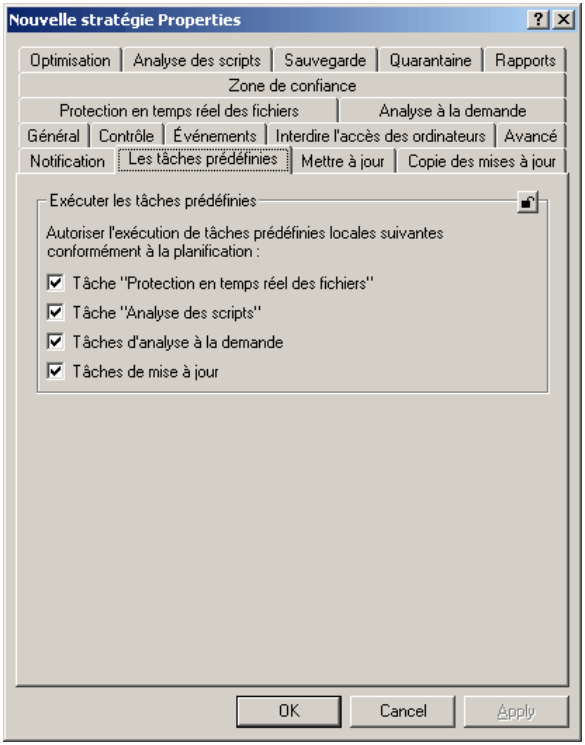

Illustration 101. Boîte de dialogue **Propriétés**, onglet **Les tâches prédéfinies**

4. Désélectionnez la case en regard de la tâche prédéfinie dont vous souhaitez désactiver l'exécution programmée.

   Pour rétablir la programmation de la tâche prédéfinie, cochez à nouveau la case.

5. Cliquez sur **OK**.

Remarque

Si vous souhaitez désactiver le lancement programmé des tâches prédéfinies, vous pouvez les lancer manuellement depuis la console de Kaspersky Anti-Virus dans MMC ou de la console d'administration Kaspersky Admnistration Kit.

CHAPITRE 20. CONFIGURATION DE KASPERSKY ANTI-VIRUS DANS LA BOITE DE DIALOGUE PARAMETRES DE L'APPLICATION

Le présent chapitre aborde les sujets suivants :

- Configuration des paramètres de Kaspersky Anti-Virus (cf. point 20.2, p. 303) ;
- Blocage de l'accès depuis les ordinateurs (cf. point 20.3, p. 307) ;
- Administration des objets en quarantaine et configuration de la quarantaine (cf. point 20.4, p. 317) ;
- Administration des fichiers de la sauvegarde et configuration de celle-ci (cf. point 20.5, p. 320) ;
- Configuration des notifications relatives aux événements de Kaspersky Anti-Virus envoyées à l'administrateur et aux utilisateurs (cf. point 20.6, p. 322) ;
- Administration de la zone de confiance (cf. point 20.7, p. 325).

Pour voir comment ouvrir la boîte de dialogue **Paramètres de l'application**, consultez le point 20.1 à la page 301.

20.1. Boîte de dialogue *Paramètres de l'application*

La boîte de dialogue **Paramètres de l'application** vous permet d'administrer Kaspersky Anti-Virus à distance et de le configurer sur le serveur protégé sélectionné.

*Pour ouvrir la boîte de dialogue **Paramètres de l'application** :*

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés : <nom de l'ordinateur>**, sur l'onglet **Applications**, sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** dans la liste des applications installées (cf. ill. 102) puis, cliquez sur **Propriétés**.

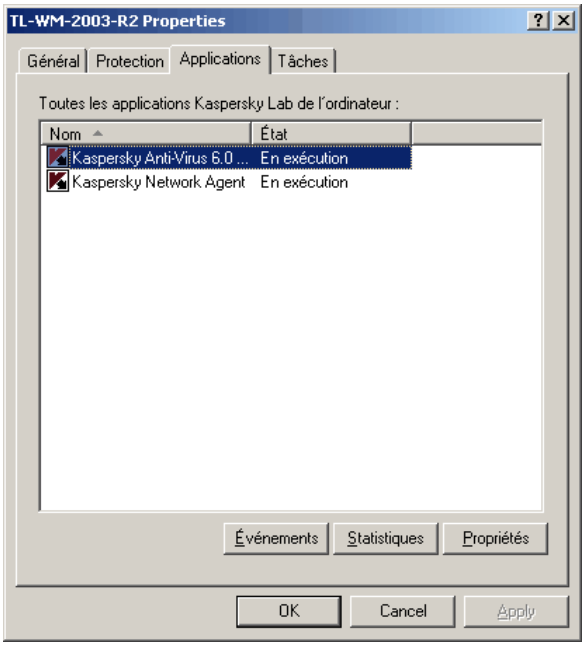

Illustration 102. Liste des logiciels antivirus dans la boîte de dialogue **Propriétés : <nom de l'ordinateur>**

La boîte de dialogue **Propriétés de l'application** s'ouvre (cf. ill. 103).

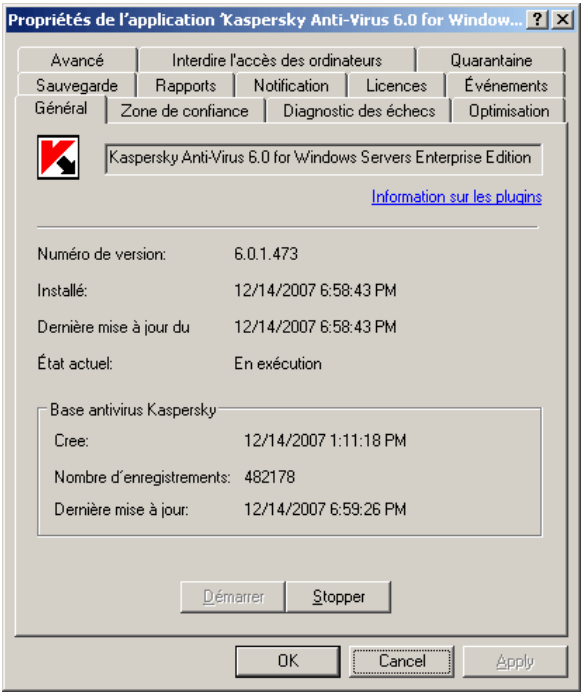

Illustration 103. Boîte de dialogue **Propriétés de l'application**, onglet **Général**

Remarque

Pendant l'application de la stratégie de Kaspersky Administration Kit, les valeurs des paramètres accompagnés dans la stratégie de l'icône dans la boîte de dialogue **Propriétés de l'application** de la console d'administration ne peuvent être modifiés.

20.2. Configuration des paramètres généraux de Kaspersky Anti-Virus

Pour configurer les paramètres généraux de Kaspersky Anti-Virus :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).

Sur les onglets suivants, modifiez la valeur des paramètres généraux de Kaspersky Lab en fonction de vos besoins.

- Sur l'onglet **Optimisation** (cf. ill. 104) :
  - Définissez le nombre maximum de processus de travail que Kaspersky Anti-Virus peut lancer (cf. ill. B.1.1, p. 377) ;
  - Définissez le nombre de processus fixe pour les tâches de la protection en temps réel (cf. point B.1.2, p. 378) ;
  - Définissez le nombre maximum de processus pour les tâches d'analyse à la demande en arrière-plan (cf. point B.1.3, p. 379) ;
  - Définissez le nombre de tentatives de restauration des tâches après leur arrêt accidentel (cf. point B.1.4, p. 380).

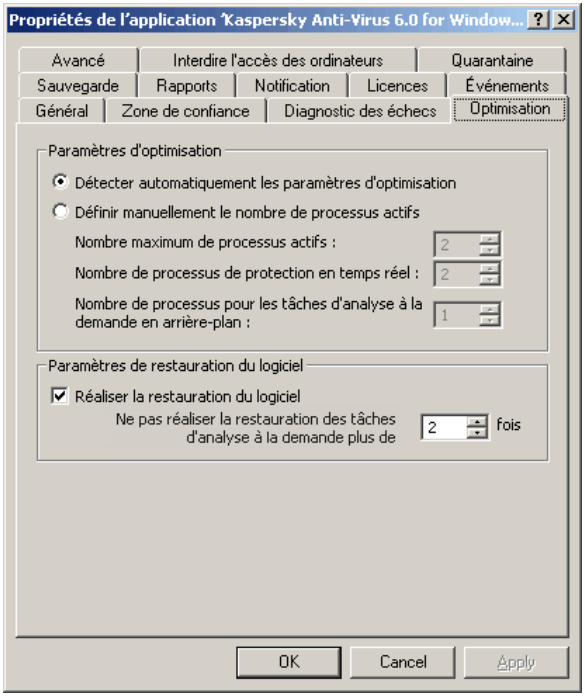

Illustration 104. Boîte de dialogue **Propriétés de l'application**, onglet **Optimisation**

- Sur l'onglet **Avancé** (cf. ill. 105) :

- Indiquez si l'icône de Kaspersky Anti-Virus doit s'afficher dans la zone de notification de la barre des tâches du serveur chaque fois que Kaspersky Anti-Virus sera lancé automatiquement après le redémarrage du serveur (pour en savoir plus sur l'icône de Kaspersky Anti-Virus, consultez le point 2.4 à la page 36) ;
- Indiquez la durée (en jours) pendant laquelle les rapports de synthèse et détaillés sur l'exécution des tâches et repris dans la console de Kaspersky Anti-Virus dans MMC dans le noeud **Rapports** seront conservés (cf. point B.1.5, p. 381) ;
- Indiquez la durée de conservation, en jours, des informations affichées dans la console de Kaspersky Anti-Virus dans MMC dans le noeud **Enregistrement d'audit système** (cf. point B.1.6, p. 382) ;
- Indiquez les actions exécutées par Kaspersky Anti-Virus en cas d'alimentation du serveur par la batterie (cf. B.1.7, p. 383) ;
- Définir le nombre de jours après lequel les événements *La base de données n'est plus à* jour, *La base de données est périmée* et *L'analyse complète de l'ordinateur n'a pas été réalisée depuis longtemps* sont déclenchés (cf. point B.1.8 p. 383).

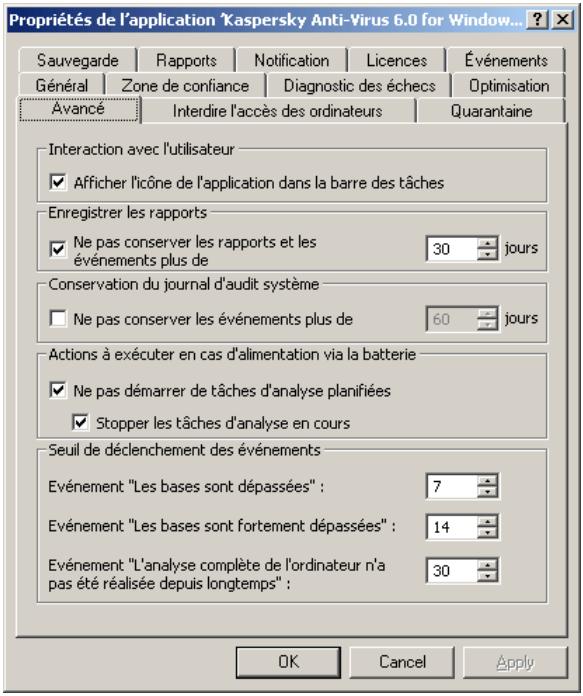

Illustration 105. Boîte de dialogue **Paramètres de l'application**, onglet **Avancé**

- Sur l'onglet **Diagnostic des échecs** (cf. ill. 106) :
  - Activez ou désactivez la constitution d'un journal de traçage ; si la constitution de ce journal est activée, configurez les paramètres du journal (cf. point B.1.9, p. 384) ;
  - Activez ou désactivez la création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (cf. point B.1.10, p. 390).

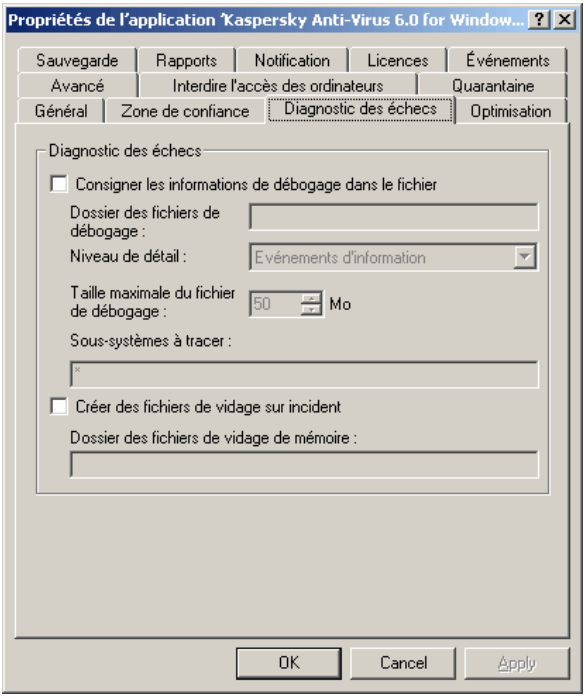

Illustration 106. Boîte de dialogue **Propriétés de l'application**, onglet **Diagnostic des échecs**

2. Une fois que vous avez modifié les valeurs des paramètres requis de Kaspersky Anti-Virus, cliquez sur le bouton **OK**.

20.3. Interdiction de l'accès des ordinateurs

La boîte de dialogue **Propriétés de l'application** vous permet d'administrer l'interdiction de l'accès des ordinateurs et d'éviter ainsi les épidémies de virus (pour de plus amples informations, consultez le point 7.1 à la page 97).

Vous pouvez exécuter les opérations suivantes :

- Activer ou désactiver l'interdiction automatique de l'accès des ordinateurs (cf. point 20.3.1, p. 308) ;

- Configurer les paramètres d'interdiction automatique de l'accès des ordinateurs (cf. point 20.3.1, p. 308) ;
- Ajouter des ordinateurs à la liste des exclusions de l'interdiction (cf. point 20.3.3, p. 311) ;
- Activer le renforcement automatique du niveau de protection si le nombre d'ordinateurs bloqués atteint la valeur seuil (fonction *Prévention des épidémies virales*) (cf. point 20.3.4, p. 312) ;
- Consulter la liste des interdictions d'accès (cf. point 20.3.5, p. 313) ;
- Interdire manuellement l'accès des ordinateurs (cf. point 20.3.6, p. 315) ;
- Octroyer l'accès des ordinateurs (cf. point 20.3.7, p. 316).

20.3.1. Activation ou désactivation de l'interdiction automatique d'accès des ordinateurs

Pour en savoir plus sur la fonction de l'interdiction automatique de l'accès des ordinateurs, lisez le point B.4.1 à la page 417.

Remarque

Si vous activez la fonction d'interdiction automatique de l'accès des ordinateurs, elle sera effective uniquement lors de l'exécution de la tâche **Protection en temps réel des fichiers**.

Pour activer ou désactiver la fonction d'interdiction d'accès des ordinateurs :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Sur l'onglet **Interdire l'accès des ordinateurs** (cf. ill. 107), réalisez les actions suivantes :
   - Pour activer l'interdiction automatique de l'accès des ordinateurs, cochez la case **Activer l'interdiction d'accès des ordinateurs au serveur** ;
   - Pour désactiver l'interdiction automatique de l'accès des ordinateurs, désélectionnez la case **Activer l'interdiction d'accès des ordinateurs au serveur**.

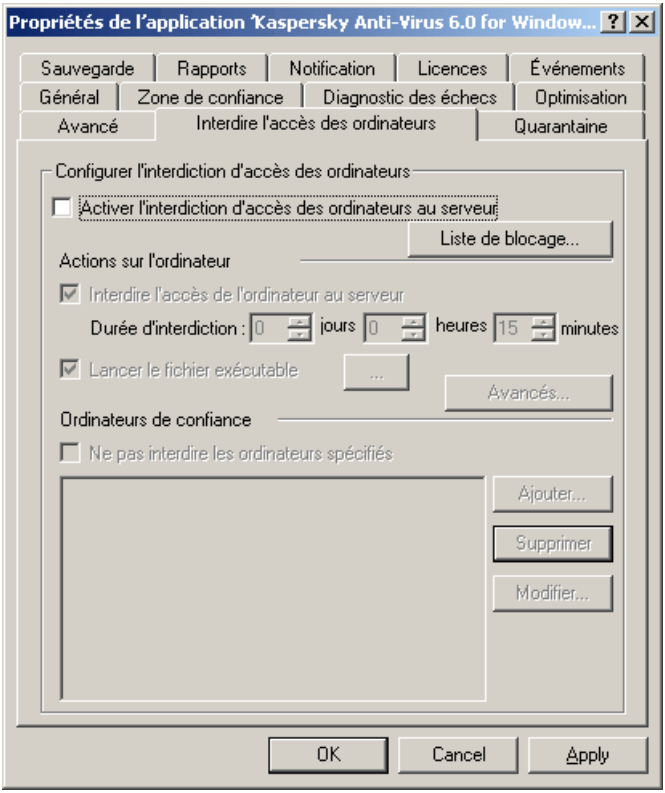

Illustration 107. Boîte de dialogue **Propriétés de l'application**, onglet **Interdire l'accès des ordinateurs**

20.3.2. Configuration des paramètres d'interdiction automatique de l'accès des ordinateurs

Pour configurer les paramètres d'interdiction automatique de l'accès des ordinateurs :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).

2. Assurez-vous que la case **Activer l'interdiction d'accès des ordinateurs au serveur** de l'onglet **Interdire l'accès des ordinateurs** est cochée (B.4.1 à la page 417).

3. Dans le groupe de paramètres **Actions sur l'ordinateur**, sélectionnez les actions que Kaspersky Anti-Virus exécutera lors des tentatives d'écriture d'un objet infecté ou potentiellement infecté sur le serveur depuis un ordinateur (B.4.2 à la page 417).

   - Si vous avez sélectionné **Interdire l'accès de l'ordinateur au serveur**, définissez la durée de la période (en jours, heures ou minutes) pendant laquelle vous souhaitez interdire l'accès des ordinateurs indiqués.
   - Si vous avez sélectionné l'option **Lancer le fichier exécutable**, cliquez sur le bouton de la liste ... et dans la boîte de dialogue **Fichier exécutable** (cf. ill. 108), indiquez le fichier exécutable (son nom ou le chemin d'accès complet) ainsi que le compte utilisateur sous les privilèges duquel le fichier exécutable sera lancé.

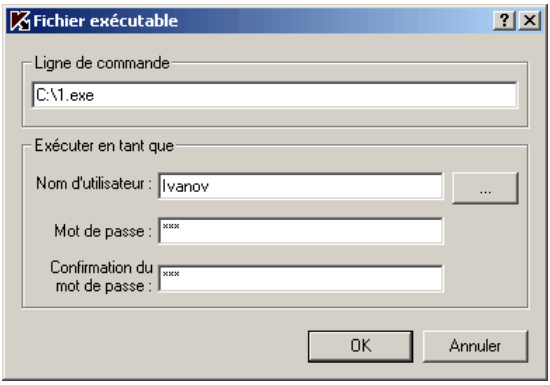

Illustration 108. Boîte de dialogue **Fichier exécutable**

4. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

20.3.3. Exclusion d'ordinateurs de l'interdiction (ordinateurs de confiance)

Pour ajouter un ordinateur à la liste des exclusions de l'interdiction (cf. point B.4.3, p. 419) :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Assurez-vous que la case **Activer l'interdiction d'accès des ordinateurs au serveur** de l'onglet **Interdire l'accès des ordinateurs** est cochée (cf. point B.4.1, p. 417).
3. Dans le groupe de paramètres **Ordinateurs de confiance**, cochez la case **Ne pas interdire les ordinateurs spécifiés** et exécutez les actions suivantes :
   a) Cliquez sur le bouton **Ajouter** et sélectionnez l'ordinateur dans la boîte de dialogue **Ajouter un ordinateur** (cf. ill. 109). Exécutez une des actions suivantes :
      - Sélectionnez **Utiliser le nom réseau d'ordinateur** et indiquez le nom NetBIOS de l'ordinateur ;
      - Indiquez l'adresse IP unique : Sélectionnez **Utiliser l'adresse IP réseau** et saisissez l'adresse IP de l'ordinateur ;
      - Indiquez la plage d'adresses IP : **Utiliser une plage d'adresses IP**. Saisissez la première adresse IP de la plage dans le champ **Adresse IP initiale** et la dernière adresse IP dans le champ **Adresse IP finale**. Tous les ordinateurs dont l'adresse IP appartient à la plage définie seront considérés comme des ordinateurs de confiance.

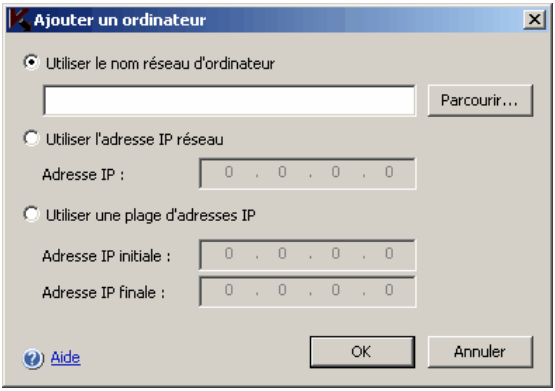

Illustration 109. Boîte de dialogue **Ajouter un ordinateur**

b) Cliquez sur **OK**.

4. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

20.3.4. Prévention des épidémies virales

Vous pouvez utiliser la fonction *Préventions des épidémies virales*. Lorsque cette fonction est activée, Kaspersky Anti-Virus augmente automatiquement le niveau de sécurité dès que le nombre d'ordinateurs bloqués atteint le seuil défini.

La fonction *Prévention des épidémies virales* est décrite au point B.4.4 à la page 419.

Pour activer/désactiver la fonction Prévention des épidémies virales :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Assurez-vous que la case **Activer l'interdiction d'accès des ordinateurs au serveur** de l'onglet **Interdire l'accès des ordinateurs** est cochée.
3. Cliquez sur **Avancé**.
4. Dans la boîte de dialogue **Avancé** (cf. ill. 110), exécutez une des actions suivantes.
   - Pour activer la fonction Prévention des épidémies virales :
     a) Cochez la case **Augmenter le niveau de protection si le nombre d'ordinateurs dépasse** ;

b) Définissez le nombre d'ordinateurs interdits dans la liste qui, une fois atteint, entraînera le renforcement de la protection offerte par Kaspersky Anti-Virus ;

c) Activez ou désactivez le rétablissement du niveau de sécurité lorsque le nombre d'ordinateurs dont l'accès au serveur est interdit revient au niveau indiqué. Précisez le nombre d'ordinateurs dans le champ **Rétablir le niveau de protection si le nombre d'ordinateurs est inférieur à**.

- Pour désactiver la fonction Prévention des épidémies de virus, désélectionnez la case **Augmenter le niveau de protection si le nombre d'ordinateurs dépasse**.

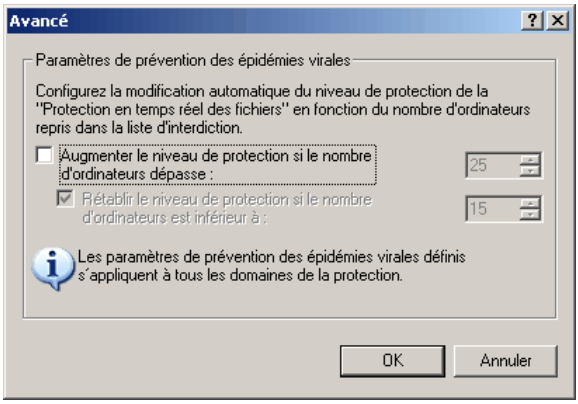

Illustration 110. Boîte de dialogue **Avancé**

5. Cliquez sur **OK**.
6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

20.3.5. Consultation de la liste des accès interdits au serveur

Attention !

Les ordinateurs repris dans la liste des accès interdits au serveur ne peuvent accéder au serveur protégé uniquement lorsque la tâche **Protection en temps réel des fichiers** est exécutée et que l'interdiction automatique de l'accès des ordinateurs est activée.

Pour consulter la liste des ordinateurs qui ne peuvent accéder pour l'instant au serveur protégé :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Cliquez sur le bouton **Liste d'interdiction** dans l'onglet **Interdire l'accès des ordinateurs** (cf. ill. 111).

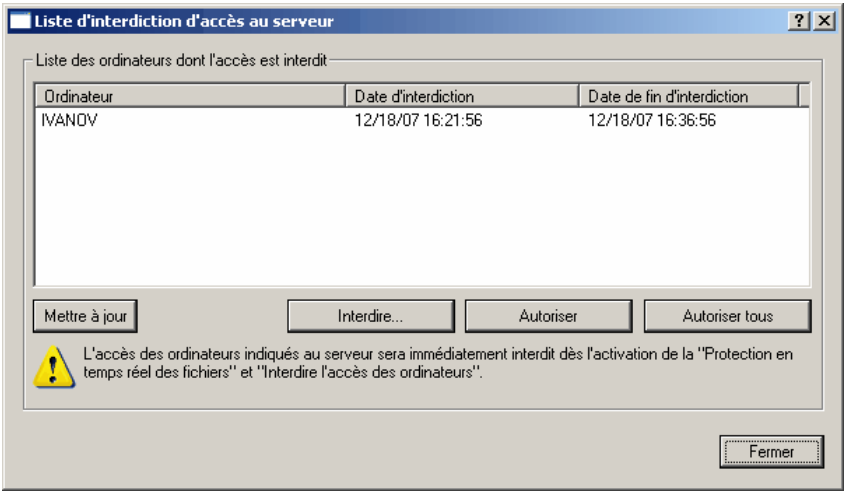

Illustration 111. Boîte de dialogue **Liste de blocage de l'accès au serveur**

La boîte de dialogue **Liste d'interdiction d'accès au serveur** reprend les informations suivantes relatives aux ordinateurs qui ne peuvent actuellement accéder au serveur protégé :

Champ	Description
Ordinateur	Informations relatives à l'ordinateur dans la liste d'interdiction (nom de réseau, adresse IP).
Date d'interdiction	Date et heure où l'ordinateur a été interdit ; ces données sont affichées selon les paramètres de la configuration régionale de Microsoft Windows de l'ordinateur où est installée la console d'administration.

Champ	Description
Date de fin d'interdiction	Date et heure où l'ordinateur ne sera plus bloqué ; ces données sont affichées selon les paramètres de la configuration régionale de Windows de l'ordinateur où est installée la console console d'administration.

20.3.6. Interdiction manuelle de l'accès des ordinateurs

Si vous savez qu'un ordinateur de l'intranet est infecté, vous pouvez l'empêcher manuellement d'accéder au serveur protégé.

Attention !

Les ordinateurs repris dans la liste d'interdiction d'accès au serveur ne peuvent accéder au serveur protégé uniquement lorsque la tâche **Protection en temps réel des fichiers** est exécutée et que l'interdiction automatique de l'accès des ordinateurs est activée.

Pour interdire l'accès de l'ordinateur au serveur :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Cliquez sur le bouton **Liste d'interdiction** dans l'onglet **Interdire l'accès des ordinateurs**.
3. Cliquez sur le bouton **Bloquer** dans la boîte de dialogue **Liste d'interdiction**.
4. Dans la boîte de dialogue **Interdiction de l'accès de l'ordinateur** (cf. ill. 112), indiquez le nom de réseau de l'ordinateur que vous souhaitez bloquer.

Remarque

Dans le champ **Nom de l'ordinateur**, saisissez uniquement les noms de réseau NetBIOS des ordinateurs et pas les adresses DNS.

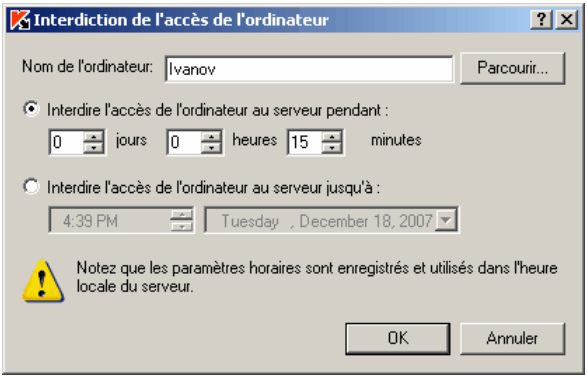

Illustration 112. Boîte de dialogue **Interdiction de l'accès de l'ordinateur**

5. Exécutez ensuite une des actions suivantes :
   - Sélectionnez **Interdire l'accès de l'ordinateur au serveur pendant** et définissez l'intervalle de temps pendant lequel vous souhaitez empêcher l'accès de l'ordinateur au serveur ;
   - Sélectionnez **Interdire l'accès de l'ordinateur au serveur jusqu'à** pour définir la date et l'heure de la fin de l'interdiction de l'accès de l'ordinateur.

   Remarque

   Indiquez la date et l'heure en fonction de la date et de l'heure affichée par le serveur protégé.
6. Cliquez sur **OK**.
7. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

20.3.7. Levée de l'interdiction de l'accès des ordinateurs

Pour autoriser l'accès d'un ordinateur :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. Cliquez sur le bouton **Liste d'interdiction** dans l'onglet **Interdire l'accès des ordinateurs**.

3. La boîte de dialogue **Liste d'interdiction** présente la liste des ordinateurs bloqués parmi lesquels vous devrez sélectionner l'ordinateur que vous souhaitez débloquer avant de cliquer sur le bouton **Autoriser l'ordinateur**.

   Afin de débloquer en une fois tous les ordinateurs bloqués, cliquez sur le bouton **Autoriser tous**.

4. Cliquez sur **OK**.

5. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

20.4. Administration des objets en quarantaine et configuration de la quarantaine

20.4.1. Fonctions de quarantaine et leur configuration

Le tableau ci-après énumère les fonctions de la quarantaine et les outils d'administration qui vous permettent de gérer ces fonctions.

Tableau 27. Fonctions de quarantaine et leur configuration

Fonction de la quarantaine	Console d'administration de Kaspersky Administration Kit	Console de Kaspersky Anti-Virus dans MMC
Consultation, tri et suppression des objets	Oui (cf. *Kaspersky Administration Kit. Manuel de l'administrateur*)	Oui
Filtrage des objets	Non	Oui
Envoi des objets suspects de la quarantaine à Kaspersky Lab pour examen	Non	Oui

Fonction de la quarantaine	Console d'administration de Kaspersky Administration Kit	Console de Kaspersky Anti-Virus dans MMC
Placement manuel des objets en quarantaine	Non	Oui
Restauration des objets de la quarantaine	Oui (uniquement dans l'emplacement d'origine)	Oui
Analyse des objets en quarantaine	Oui Lancez la tâche **Analyse des objets en quarantaine**.	Oui
Configuration des paramètres de la quarantaine	Oui Cf. point 20.4.2, p. 318.	Oui
Consultation des statistiques de la quarantaine	Oui Voir « Consultation des statistiques de Kaspersky Anti-Virus », point 18.3, p. 281.	Oui

20.4.2. Configuration de la quarantaine

La boîte de dialogue **Propriétés de l'application** du serveur protégé sélectionné vous permet de configurer les paramètres de la quarantaine.

Les informations relatives à l'isolement des objets suspects sont reprises au point 11.1 à la page 171.

Pour configurer les paramètres de la quarantaine :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301).
2. En fonction des besoins, vous pouvez modifier les paramètres suivants sur l'onglet **Quarantaine** (cf. ill. 113) :

- Pour désigner un autre répertoire de quarantaine, sélectionnez le répertoire voulu sur le disque ou saisissez le chemin d'accès complet dans le champ **Répertoire de quarantaine** (cf. point B.6.1, p. 435) ;
- Pour indiquer la taille maximale de la quarantaine, cochez la case **Taille maximale de la quarantaine** et saisissez la valeur souhaitée en mégaoctets (cf. point B.6.2, p. 436) ;
- Pour indiquer le seuil d'espace disponible minimum dans la quarantaine, cochez la case **Taille maximale de la quarantaine**, cochez la case **Seuil d'espace libre** et saisissez la valeur souhaitée en mégaoctets (cf. point B.6.3, p. 436) ;
- Pour désigner un autre répertoire de restauration des objets, sélectionnez, dans le groupe de paramètres **Paramètres de restauration**, le répertoire souhaité sur le disque ou saisissez son chemin d'accès complet (cf. point B.6.4, p. 437).

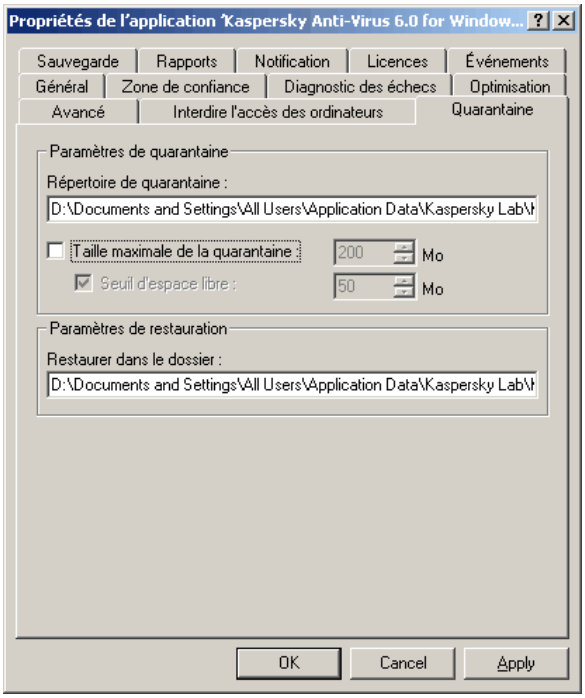

Illustration 113. Boîte de dialogue **Propriétés de l'application**, onglet **Quarantaine**

3. Cliquez sur **OK**.

20.5. Administration des fichiers de la sauvegarde et configuration de celle-ci

20.5.1. Fonctions de la sauvegarde et moyens de configuration

Le tableau ci-après énumère les fonctions de la sauvegarde et les outils d'administration qui vous permettent de gérer ces fonctions.

Tableau 28. Fonctions de la sauvegarde

Fonction de la sauvegarde	Console d'administration de Kaspersky Administration Kit	Console de Kaspersky Anti-Virus dans MMC
Consultation, tri et suppression des fichiers	Oui	Oui
Filtrage des fichiers	Non	Oui
Restauration des fichiers depuis la sauvegarde	Oui (uniquement dans l'emplacement d'origine)	Oui
Configuration des paramètres de la sauvegarde	Oui Cf. point 20.5.2, p. 321.	Oui
Consultation des statistiques de la sauvegarde	Oui Voir « Consultation des statistiques de Kaspersky Anti-Virus », point 18.3, p. 281.	Oui

20.5.2. Configuration des paramètres de la sauvegarde

La boîte de dialogue **Propriétés de l'application** du serveur protégé sélectionné vous permet de configurer les paramètres de la sauvegarde.

Pour en savoir plus sur la création des copies de sauvegarde des objets avant leur réparation ou leur suppression, lisez le point 12.1 à la page 190.

Pour configurer les paramètres de la sauvegarde :

1. Ouvrez la boîte de dialogue **Propriétés de l'application** (cf. point 20.1, p. 301) et sélectionnez l 'onglet **Sauvegarde**.
2. Sur l'onglet **Sauvegarde**, configurez les paramètres du dossier de sauvegarde en fonction de vos besoins (cf. ill. 114) :
   - Pour désigner un nouvel emplacement pour la sauvegarde, sélectionnez le répertoire voulu ou saisissez son chemin d'accès complet dans le champ **Dossier de sauvegarde** (cf. point B.7.1, p. 438) ;
   - Pour modifier la taille maximale du dossier de quarantaine, cochez la case **Taille max. du dossier de sauvegarde** et saisissez la valeur souhaitée en mégaoctets (cf. point B.7.2, p. 439) ;
   - Pour modifier le seuil d'espace disponible minimum dans le dossier de sauvegarde, cochez la case **Taille max. du dossier de sauvegarde**, cochez la case **Seuil d'espace libre** et saisissez la valeur souhaitée en mégaoctets (cf. point B.7.3, p. 440) ;
   - Pour désigner un autre répertoire de restauration des objets, sélectionnez, dans le groupe de paramètres **Paramètres de restauration**, le répertoire souhaité sur le disque ou saisissez son chemin d'accès complet (cf. point B.7.4, p. 441).

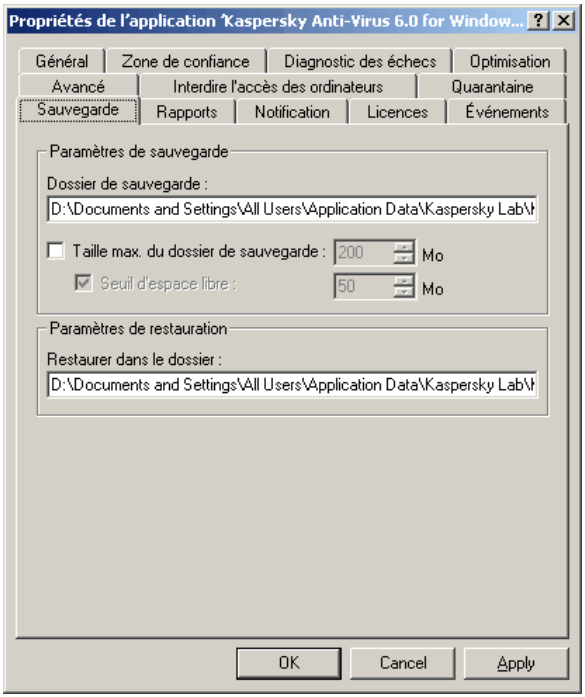

Illustration 114. Boîte de dialogue **Propriétés de l'application**, onglet **Sauvegarde**

3. Cliquez sur **OK**.

20.6. Configuration des notifications

Cette section aborde les sujets suivants :

- Les informations générales sur la configuration des notifications via la console d'administration (cf. point 20.6.1, p. 322) ;
- Configuration des notifications envoyées à l'administrateur et aux utilisateurs sur l'onglet *Notification* (cf. point 20.6.1, p. 322).

20.6.1. Informations générales

Dans la console d'administration de Kaspersky Administration Kit, vous pouvez configurer les notifications adressées à l'administrateur et aux utilisateurs rela-

tives aux événements liés à l'utilisation de Kaspersky Anti-Virus et à l'état de la protection du serveur protégé :

- L'administrateur peut obtenir des informations sur les événements de certains types ;
- Les utilisateurs du réseau local qui accèdent au serveur protégé peuvent obtenir des informations sur les événements de type *Menace découverte* et *L'ordinateur a été ajouté à la liste d'interdiction* ; les utilisateurs du serveur via le terminal peuvent obtenir des informations sur les événements *Une menace a été découverte*.

Vous pouvez configurer les notifications relatives aux événements de Kaspersky Anti-Virus pour un serveur dans la fenêtre **Propriétés de l'application** du serveur sélectionné ou pour un groupe de serveurs dans la fenêtre **Paramètres de stratégie** du groupe sélectionné.

Dans ces boîtes de dialogue, vous pouvez configurer les notifications sur l'onglet **Événements** ou sur l'onglet **Notification**.

- L'onglet **Événements** (onglet standard de Kaspersky Administration Kit) vous permet de configurer les notifications adressées à l'administrateur sur les événements de certains types. Pour connaître les modes de notification que vous pouvez configurer et la marche à suivre, consultez le document *Kaspersky Administration Kit. Manuel de l'administrateur* ;
- L'onglet **Notification** vous permet de configurer les notifications adressées à l'administrateur et aux utilisateurs. Pour en savoir plus sur les modes de notification que vous pouvez configurer sur l'onglet **Notification**, consultez le point 15.1 à la page 236. Pour voir comment configurer les notifications sur l'onglet **Notification**, consultez le point 20.6.1 à la page 322.

Les notifications relatives à certains types d'événements peuvent être configurées uniquement sur un des onglets tandis que d'autres notifications peuvent être configurées sur les deux.

Remarque

Si vous configurez les notifications relatives aux événements d'un type d'une manière sur les deux onglets, à savoir **Événements** et **Notification**, alors l'administrateur recevra les notifications relatives à ces événements deux fois de cette manière.

20.6.2. Configuration des notifications adressées à l'administrateur et aux utilisateurs sur l'onglet *Notification*

Pour configurer les notifications :

1. Ouvrez la boîte de dialogue **Propriétés de l'application**(cf. point 20.1, p. 301) et sélectionnez l 'onglet **Notification**.
2. Sur l'onglet **Notification** (cf. ill. 115), configurez les notifications relatives aux événements du type requis puis, cliquez sur le bouton **OK**.

La configuration des notifications sur l'onglet **Notification** est identique à la configuration de notifications dans la boîte de dialogue **Notifications** de la console de Kaspersky Anti-Virus dans MMC. Pour en savoir plus sur la manière de procéder à la configuration, consultez le point 15.2 à la page 238.

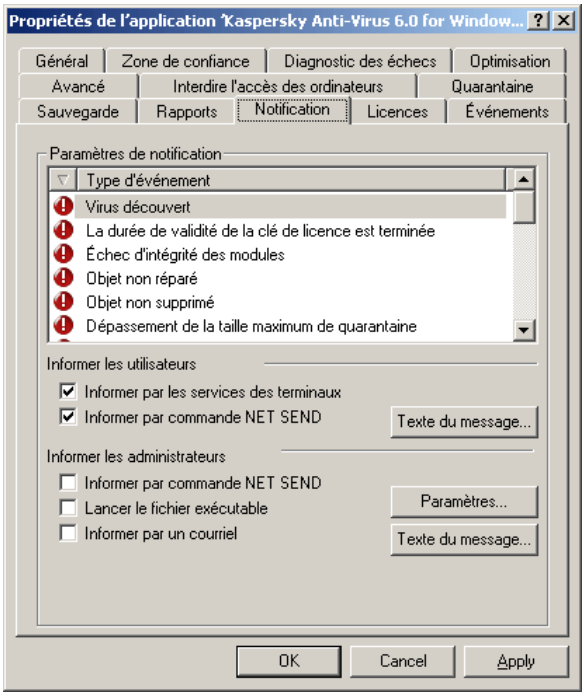

Illustration 115. Boîte de dialogue **Paramètres de l'application**, onglet **Notification**

20.7. Administration de la zone de confiance

Cette rubrique aborde les points suivants :

- Ajout de processus à la liste des processus de confiance (cf. point 20.7.1 , p. 325) ;
- Désactivation de la protection en temps réel des fichiers durant la copie de sauvegarde (cf. point 20.7.2, p. 327) ;
- Ajout d'exclusion (cf. point 20.7.3, p. 329) ;
- Application à la zone de confiance (cf. point 20.7.4, p. 332).

Pour en savoir plus sur la zone de confiance de Kaspersky Anti-Virus, lisez le point 8.1 à la page 109.

20.7.1. Ajout de processus à la liste des processus de confiance

La console d'administration de Kaspersky Administration Kit vous permet d'ajouter les fichiers exécutables des processus sur le disque du serveur protégé à la zone de confiance ; vous ne pouvez pas ajouter des processus de la liste des processus actifs sur le serveur.

Pour en savoir plus sur la zone de confiance de Kaspersky Anti-Virus, lisez le point 8.1 à la page 109.

Afin d'ajouter un processus à la liste des processus de confiance de Kaspersky Anti-Virus :

1. Ouvrez la boîte de dialogue **Propriétés de l'application**(cf. point 20.1, p. 301) et sélectionnez l 'onglet **Zone de confiance** (cf. ill. 116).
2. Activez la fonction **Processus de confiance** : cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés**.

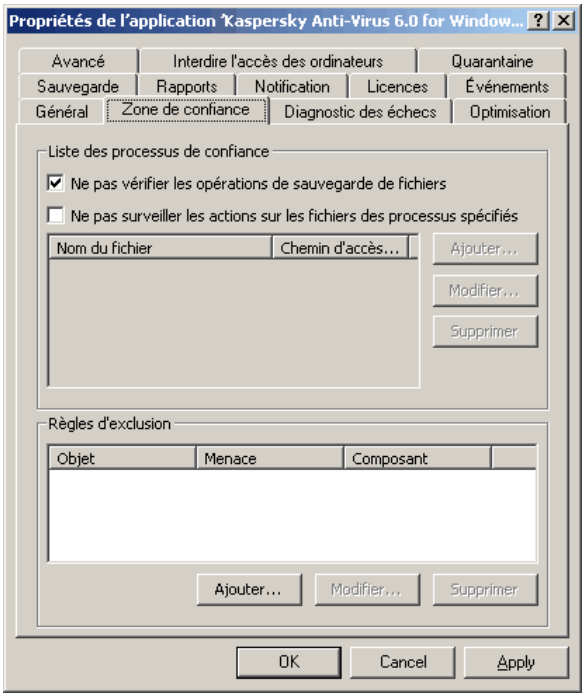

Illustration 116. Boîte de dialogue **Paramètres de l'application**, onglet **Zone de confiance**

3. Pour sélectionner le fichier exécutable du processus sur le disque du serveur protégé, procédez de la manière suivante :

   a) Cliquez sur le bouton **Ajouter** dans la boîte de dialogue **Zone de confiance** ;

   b) Dans la boîte de dialogue **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier exécutable du processus sur le disque local du serveur protégé ;

   c) Le nom du fichier et le chemin d'accès à celui-ci apparaît dans la boîte de dialogue **Ajout d'un processus de confiance** ;

      La boîte de dialogue **Ajout d'un processus de confiance** reprend le nom du fichier et le chemin d'accès à celui-ci.

   d) Cliquez sur **OK**.

Le nom du fichier exécutable du processus sélectionné apparaît dans la liste des processus de confiance de l'onglet **Zone de confiance**.

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

20.7.2. Désactivation de la protection en temps réel des fichiers durant la copie de sauvegarde

Pendant la création d'une copie de sauvegarde des fichiers, vous pouvez désactiver la protection en temps réel des fichiers sollicités durant les opérations de copie de sauvegarde. Kaspersky Anti-Virus n'analyse pas les fichiers que l'application de sauvegarde ouvre en lecteur avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Pour désactiver la protection en temps réel des fichiers durant la copie de sauvegarde :

1. Ouvrez la boîte de dialogue **Propriétés de l'application**(cf. point 20.1, p. 301) et sélectionnez l 'onglet **Zone de confiance** (cf. ill. 117).

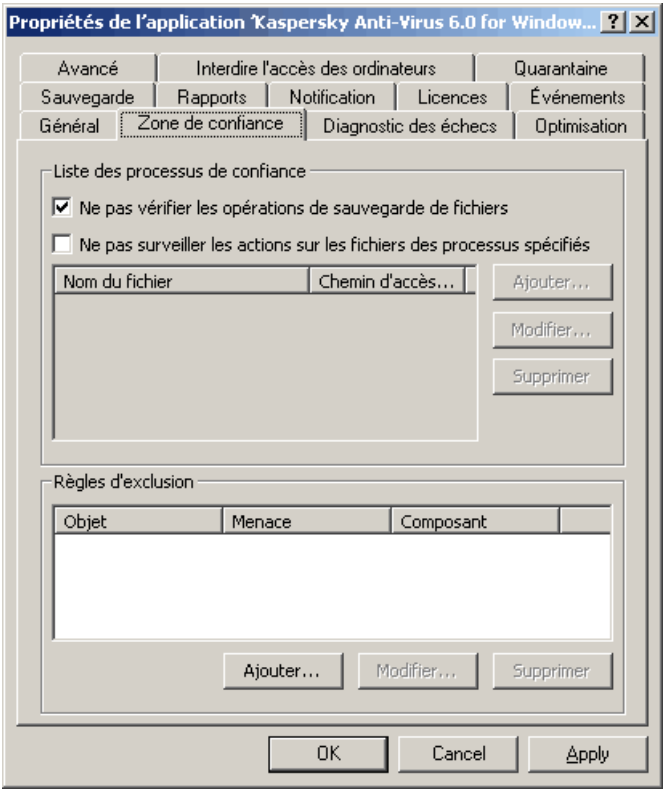

Illustration 117. Boîte de dialogue **Paramètres de l'application**, onglet **Zone de confiance**

2. Pour désactiver la protection en temps réel des fichiers sollicités pendant la copie de sauvegarde, cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.
3. Cliquez sur **OK** pour enregistrer les modifications.
4. Appliquez les exclusions à la zone de confiance dans les tâches et les stratégies sélectionnées (cf. point 20.7.4, p. 332).

20.7.3. Ajout d'exclusions à la zone de confiance

Vous pouvez ajouter des objets à la zone de confiance pour les exclure de l'analyse. Pour obtenir de plus amples informations sur la zone de confiance, lisez le point 8.1 à la page 109.

Pour ajouter une exclusion :

1. Ouvrez la boîte de dialogue **Propriétés de l'application**(cf. point 20.1, p. 301) et sélectionnez l'onglet **Zone de confiance** (cf. ill. 116).
2. Cliquez sur le bouton **Ajouter** sous le titre **Règles d'exclusion**.

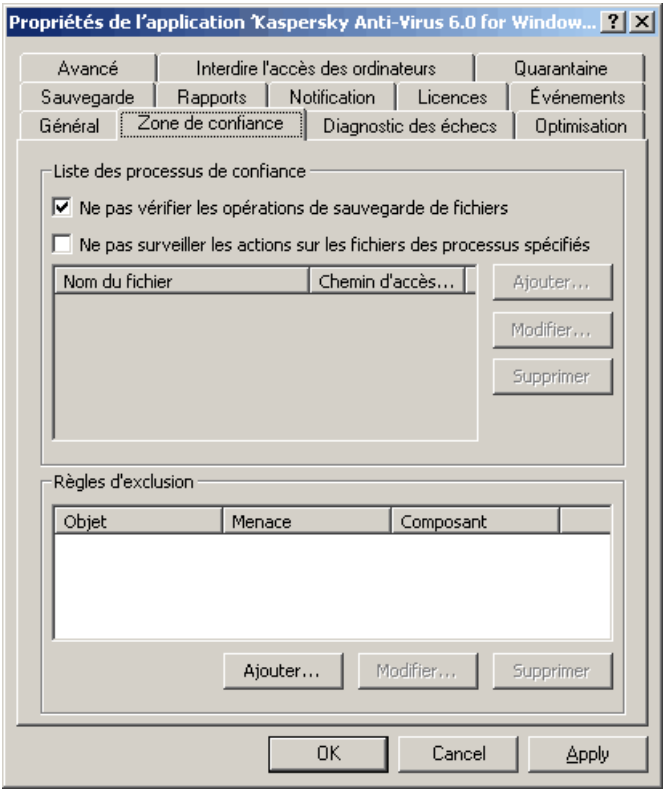

Illustration 118. Boîte de dialogue **Paramètres de l'application**, onglet **Zone de confiance**

La boîte de dialogue **Règle d'exclusion** s'ouvre.

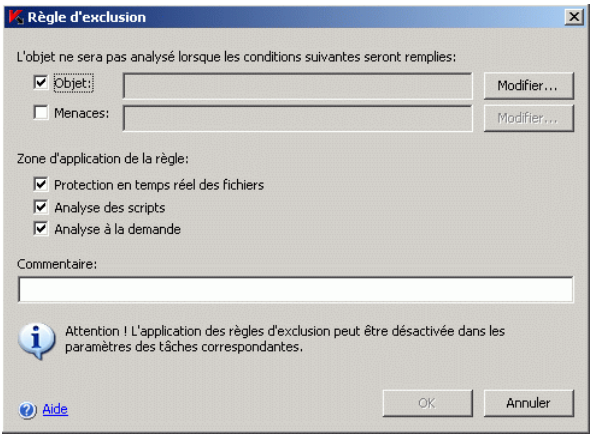

Illustration 119. Boîte de dialogue **Règle d'exclusion**

3. Indiquez la règle selon laquel Kaspersky Anti-Virus va exclure les objets.

Remarque

Pour exclure *les menaces définies dans les répertoires ou les fichiers indiqués*, cochez la case **Objet** et la case **Menaces**.

Pour exclure *toutes les menaces dans les dossiers et les fichiers indiqués*, cochez la case **Objet** et désélectionnez la case **Menaces**.

Pour exclure *les menaces définies dans toute la couverture d'analyse*, désélectionnez la case **Objet** et cochez la case **Menaces**.

- *Si vous souhaitez indiquer l'emplacement de l'objet*, cochez la case **Objet**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Sélection de l'objet**, sélectionnez l'objet qui sera exclu de l'analyse puis cliquez sur **OK** :
  - **Zone d'analyse prédéfinie**. Sélectionnez une des zones d'analyse prédéfinie dans la liste.
  - **Disque ou répertoire**. Indiquez le disque du serveur ou le répertoire sur le serveur ou dans le réseau local.
  - **Fichier**. Indiquez le fichier sur le serveur ou dans le réseau local.
  - **Fichier ou URL du script**. Désignez le script sur le serveur protégé, dans le réseau local ou sur Internet.

> **Remarque**
>
> Vous pouvez définir des masques pour les noms de répertoires ou de fichiers à l'aide des caractères génériques ? et *.

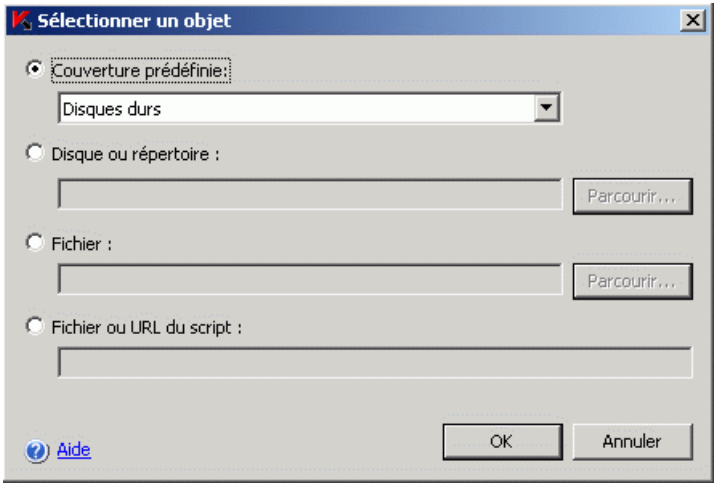

Illustration 120. Boîte de dialogue **Sélection de l'objet**

- *Si vous souhaitez définir le nom de la menace,* cochez la case **Menaces**, cliquez sur le bouton **Modifier** et dans la boîte de dialogue **Liste d'exclusion des menaces**, ajoutez les noms des menaces (pour de plus amples informations sur le paramètre, lisez le point B.3.9 à la page 411).

4. Cochez la case en regard des composants fonctionnels dans les tâches desquels la règle d'exclusion sera appliquée.
5. Cliquez sur **OK**.
   - Pour modifier une règle, sur l'onglet **Zone de confiance**, sélectionnez la règle que vous souhaitez modifier, cliquez sur le bouton **Modifier** et introduisez les modifications dans la boîte de dialogue **Règle d'exclusion**.
   - Pour supprimer une règle, sur l'onglet **Zone de confiance**, sélectionnez la règle que vous souhaitez supprimer, cliquez sur le bouton **Supprimer** et confirmer l'opération.
6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Propriétés de l'application**.

7. Le cas échéant, appliquez les exclusions à la zone de confiance dans les tâches et les stratégies sélectionnées (cf. point 20.7.4, p. 332).

20.7.4. Application de la zone de confiance

Vous pouvez activer ou désactiver l'application de la zone de confiance dans les stratégies existantes et ainsi que dans les tâches (au moment de la création de la tâche ou dans la boîte de dialogue **Propriétés de la tâche**).

Par défaut, la zone de confiance est appliquée dans toutes les tâches et les stratégies recréées.

Pour appliquer la zone de confiance dans la stratégie :

1. Dans l'arborescence de la console d'administration, déployez le nœud **Groupes** puis le groupe d'administration dont vous souhaitez configurer les paramètres de la stratégie puis déployez le nœud **Stratégies**.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la stratégie contenant les paramètres que vous souhaitez modifier puis, sélectionnez la commande **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de la stratégie**, réalisez les actions suivantes :
   - Pour appliquer les exclusions : *processus de confiance*, assurez-vous que la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** est cochée et verrouillez l'option dans le groupe de paramètres **Liste des processus de confiance** ;
   - Pour appliquer les exclusions : *opération de copie de sauvegarde,* assurez-vous que la case **Ne pas surveiller les opérations de sauvegarde des fichiers** est cochée et verrouillez l'option dans le groupe de paramètres **Liste des processus de confiance** ;
   - Pour appliquer *les exclusions définies par l'utilisateur*, verrouillez les paramètres du groupe **Exclusions**.
4. Cliquez sur **OK**.

Pour appliquer la zone de confiance dans une tâche existante :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés**.

3. Ouvrez le menu contextuel de la tâche que vous souhaitez configurer sur l'onglet **Tâches** de la fenêtre **Propriétés de l'ordinateur** puis, sélectionnez la commande **Propriétés**.

4. Dans la boîte de dialogue **Propriétés de la tâche**, onglet **Configuration**, cliquez sur le bouton **Avancé** et dans la boîte de dialogue **Avancé**, cochez la case **Tenir compte des règles de la zone de confiance**

   Vous pouvez également appliquer la zone de confiance lors de la création de la tâche.

CHAPITRE 21. CREATION ET CONFIGURATION DE TACHES

Le présent chapitre aborde les sujets suivants :

- Les tâches qui peuvent être créées dans la console d'administration (cf. point 21.1, p. 334) ;
- La création de tâches (cf. point 21.2, p. 335) ;
- La configuration des tâches (cf. point 21.3, p. 345).

21.1. Présentation de la création des tâches

Vous pouvez créer des tâches locales, d'utilisateur, de groupe ou globales des types suivants :

- Analyse à la demande ;
- Mises à jour ;
- Annulation de la mise à jour de la base de données ;
- Installation de la clé.

Vous créez les tâches locales pour le serveur protégé sélectionné dans la boîte de dialogue **Paramètres** de l'application à l'onglet **Tâches**. Les tâches de groupe sont reprise dans le noeud **Tâches de groupe** du groupe sélectionné tandis que les tâches globales sont reprises dans le noeud **Tâches globales**.

Remarque

Grâce aux stratégies, vous pouvez désactiver l'action de la planification des tâches prédéfinies locales sur tous les ordinateurs protégés appartenant à un groupe d'administration.

Les informations générales relatives aux tâches de Kaspersky Administration Kit sont reprises dans le document *Kaspersky Administration Kit. Manuel de l'administrateur*.

21.2. Création d'une tâche

Pour créer une nouvelle tâche dans la console d'administration :

1. Lancez l'Assistant de création de tâche du type requis :

   - *Pour créer une tâche locale* :

     a) Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé ;

     b) Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés** ;

     c) Sur l'onglet **Tâches**, cliquez sur le bouton **Ajouter**.

   - *Pour créer une tâche de groupe* :

     a) Dans l'arborescence de la console d'administration, sélectionnez le groupe pour lequel vous souhaitez créer une tâche de groupe ;

     b) Ouvrez le menu contextuel du sous-dossier **Tâches de groupe** et sélectionnez **Nouvelle→ tâche**.

   - *Pour créer une tâche globale* Dans l'arborescence de la console d'administration, ouvrez le menu contextuel du noeud **Tâches globales** et sélectionnez **Nouvelle → tâche**.

   La fenêtre de bienvenue de l'Assistant de création de tâche s'ouvre.

2. Dans la fenêtre **Nom de tâche** de l'Assistant de création de tâche, saisissez le nom de la tâche (100 caractères maximum, ne peut contenir les caractères **" * < > ? \ / | :)**. Il est conseillé d'inclure le type de tâche dans son nom (par exemple, (« Analyse à la demande des dossiers partagés »).

3. Dans la fenêtre **Applications**, sous le titre **Application**, sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition** et sous le titre **Type de tâche**, sélectionnez le type de tâche à créer.

4. En fonction du type de tâche créée, exécutez une des actions suivantes :

   - *Si vous créez une tâche d'analyse à la demande* :

     a) Dans la fenêtre **Couverture de l'analyse**, définissez la couverture de l'analyse.

Par défaut, la couverture de l'analyse reprend la zone **Poste de travail** (cf. ill. 121).

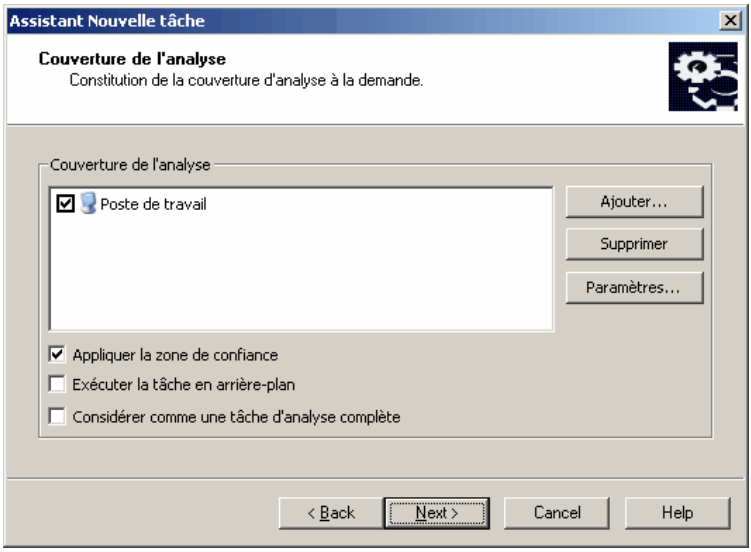

Illustration 121. Fenêtre **Couverture d'analyse** de l'Assistant de création de tâches

La couverture **Poste de travail** contient des couvertures d'analyse intégrées prédéfinies. (Ces zones sont décrites au point 9.2.1.2 à la page 125).

Si en raison des exigences de sécurité il n'est pas nécessaire d'analyser l'ensemble du serveur, vous pouvez limiter la couverture d'analyse : inclure uniquement des couvertures prédéfinies et/ou des disques, des dossiers ou des fichiers distincts.

- Pour inclure dans la zone d'analyse uniquement des zones, des disques, des dossiers ou des fichiers distincts, ouvrez la boîte de dialogue **Couverture de l'analyse** et supprimez la couverture prédéfinie **Poste de travail** puis, cliquez sur le bouton **Ajouter** et dans la boîte de dialogue **Ajout d'objets à la couverture d'analyse**, indiquez les objets qui feront partie de la couverture : sélectionnez une couverture prédéfinie dans la liste **Couverture de l'analyse prédéfinie** (cf. ill. 122), précisez le disque du serveur, le dossier ou le fichier sur le serveur ou sur un autre ordinateur dans le réseau puis, cliquez sur le bouton **OK**.

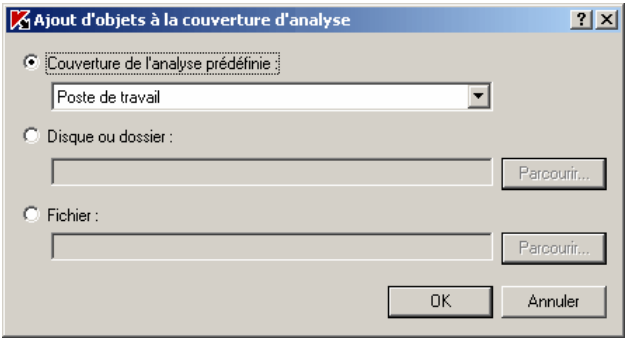

Illustration 122. Boîte de dialogue **Ajout d'objets à la couverture d'analyse**

- Pour exclure des sous-dossiers ou des fichiers de l'analyse, sélectionnez le dossier (disque) à ajouter dans la fenêtre **Paramètres** de l'Assistant puis cliquez sur le bouton **Configuration**, ensuite, dans la fenêtre **Configuration de l'analyse à la demande**, cliquez sur le bouton **Paramètres** et dans la boîte de dialogue **Configuration de la couverture de protection**, désélectionnez la case **Analyser les sous-dossiers** (**Analyser les sous-fichiers**).
- Cochez la case **Appliquer la zone de confiance** si, dans la tâche **Protection en temps réel des fichiers**, vous souhaitez exclure de l'analyse les objets décrits dans la zone de confiance de Kaspersky Anti-Virus (pour de plus amples informations sur la zone de confiance, lisez le point 8.1 à la page 109 ; pour savoir comment ajouter des exclusions à la zone de confiance dans Kaspersky Administration Kit, lisez le point 20.7 à la page 325).

b) Si vous avez l'intention d'utiliser la tâche créée en guise de tâche d'analyse complète de l'ordinateur, cochez la case **Considérer comme une tâche d'analyse complète**. Kaspersky Administration Kit évaluera l'état de la protection du serveur (des serveurs) sur la base des résultats de l'exécution de la tâche dont l'état est « Tâche d'analyse complète de l'ordinateur » et non pas sur la base des résultats de l'exécution de la tâche prédéfinie **Analyse du poste de travail**. Pour obtenir de plus amples informations sur l'octroi du statut de « tâche d'analyse complète » à la tâche d'analyse à la demande, consultez le point 21.4 à la page 347.

c) Pour attribuer au processus actif où la tâche sera exécutée la priorité de base **Bas** (**Low**), cochez la case **Exécuter la tâche en arrière-plan**. Par défaut, les processus actifs dans lesquels

les tâches de Kaspersky Anti-Virus sont exécutées ont la priorité **Moyenne** (**Normal**). La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

- *Si vous créez une des tâches de mise à jour, définissez les paramètres en fonction de vos besoins* :

  a) Sélectionnez la source des mises à jour dans la fenêtre **Source des mises à jour** (cf. point B.5.1, p. 423) ;

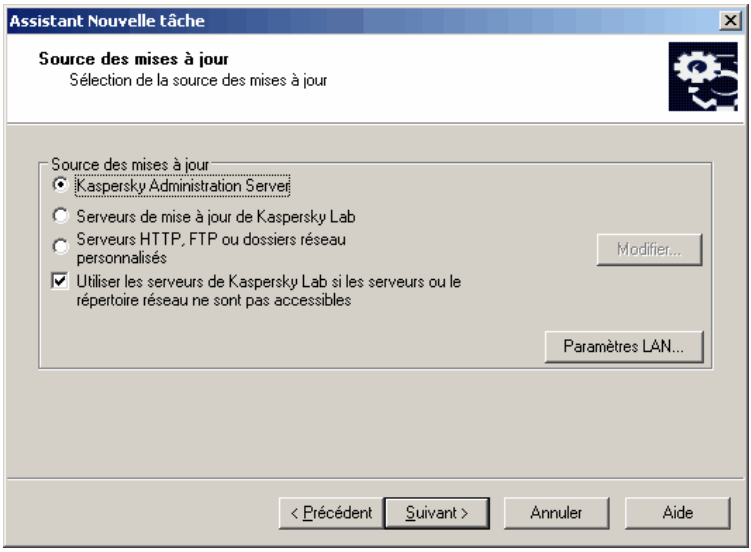

Illustration 123. Fenêtre **Source des mises à jour**

  b) Cliquez sur le bouton **Paramètres LAN**. La boîte de dialogue **Paramètres avancés** s'ouvre (cf. ill. 124) ;

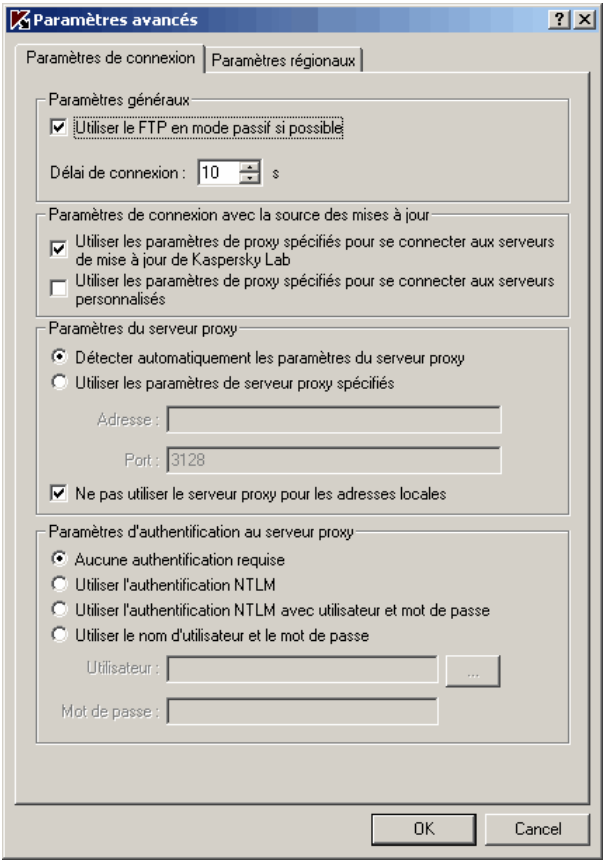

Illustration 124. Boîte de dialogue **Configuration avancée**, onglet **Configuration de la connexion**

c) Sur l'onglet **Paramètres de connexion**, réalisez les opérations suivantes :

- Précisez le mode du serveur FTP pour la connexion au serveur protégé (cf. point B.5.2, p. 424) ;
- Le cas échéant, modifiez le délai d'attente pour la connexion à la source des mises à jour (cf. point B.5.3, p. 425) ;
- Configurez les paramètres d'accès au serveur proxy pour la connexion à la source des mises à jour (cf. point B.5.4, p. 425).

d) Sur l'onglet **Paramètres régionaux**, précisez l'emplacement du serveur protégé afin d'optimaliser la réception des mises à jour (cf. point B.5.5, p. 429).

- *Si vous créez une tâche **Mise à jour des modules de l'application***, configurez les paramètres requis de la mise à jour des modules de l'application dans la fenêtre **Configuration de la mise à jour** (cf. ill. 125) :

  a) Décidez si vous souhaitez charger et installer la mise à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles (cf. point B.5.6.1, p. 431) ;

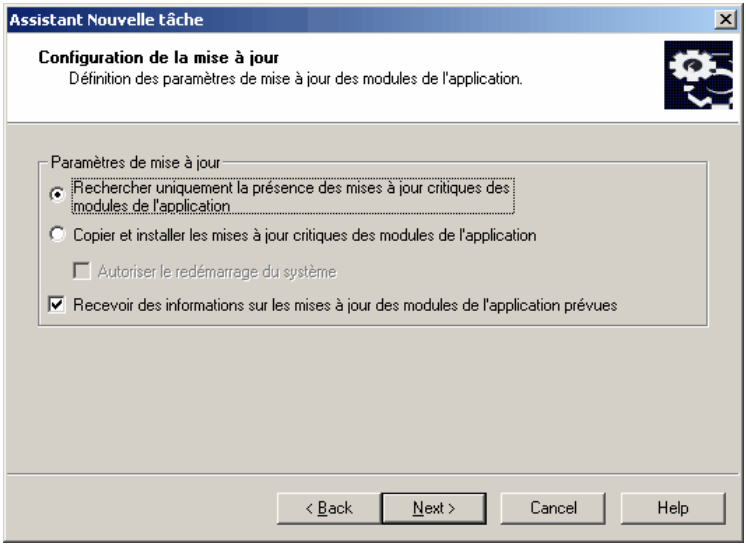

Illustration 125. Fenêtre **Configuration de la mise à jour** dans la tâche **Mise à jour des modules de l'application**

b) Si vous avez sélectionné **Copier et installer les mises à jour critiques des modules de l'application** : le redémarrage du serveur sera peut-être nécessaire pour appliquer les modules logiciels installer. Afin que Kaspersky Anti-Virus lance automatiquement le redémarrage du serveur après la fin de la tâche, cochez la case **Autoriser le redémarrage du système**. Pour annuler le redémarrage automatique après la fin de la tâche, désélectionnez la case **Autoriser le redémarrage du système** ;

c) Si vous souhaitez obtenir des informations sur la diffusion des mises à jour prévues des modules de l'application, cochez la

case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez configurer les notifications adressées à l'administrateur pour l'événement *Des mises à jour prévues des modules de Kaspersky Anti-Virus sont disponibles*. Cette notification reprend l'adresse des pages de notre site d'où les mises à jour prévues pourront être téléchargées (pour de plus amples informations sur la configuration des notifications, consultez le point 15.2 à la page 238).

- *Si vous créez une tâche* ***Copie des mises à jour***, précisez la composition des mises à jour (cf. point B.5.7.1, p. 432) ainsi que le dossier où elles seront enregistrées (cf. point B.5.7.2, p. 434) dans la fenêtre **Paramètres de copie des mises à jour** des mises à jour.

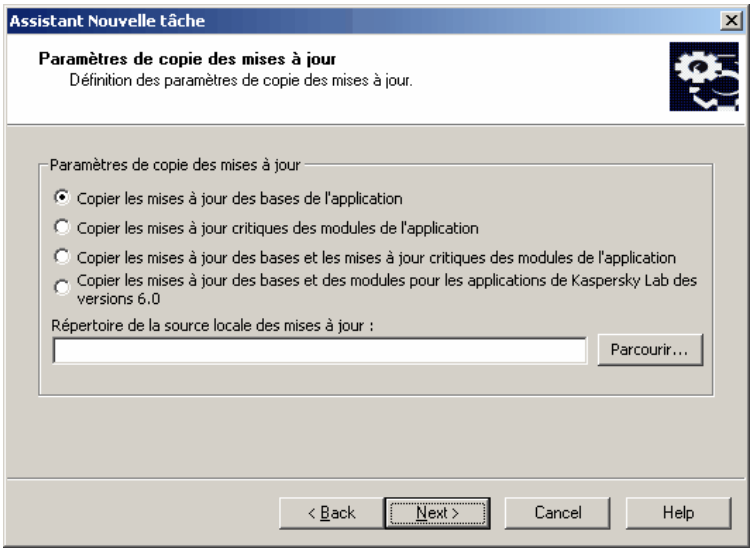

Illustration 126. Fenêtre **Paramètres de copie des mises à jour**

- *Si vous créez une tâche* ***Installation de clé de licence***, indiquez le nom du fichier de clé (extension .key) et le chemin d'accès complet à celui-ci dans le champ **Clé** de la fenêtre **Installation de la clé de licence** (cf. ill. 127).

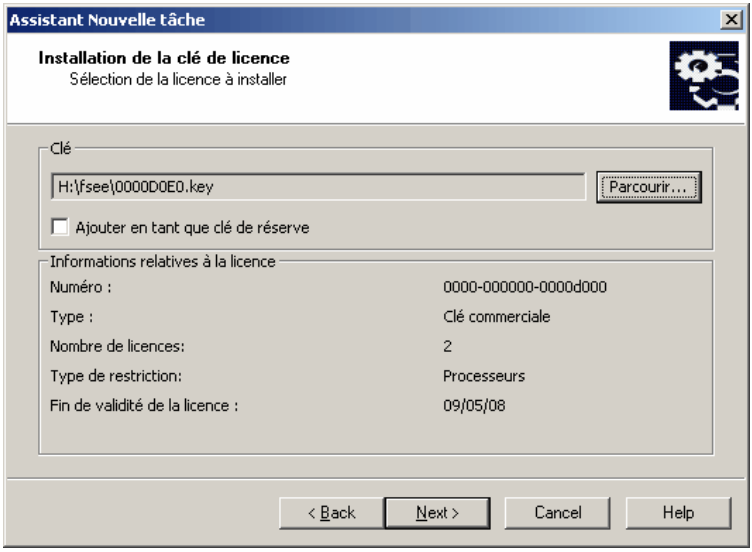

Illustration 127. Fenêtre **Installation de la clé de licence**

5. Configurez les paramètres requis de planification de la tâche (vous pouvez configurer la planification des tâches de tous les types à l'exception des tâches **Installation de clé de licence** et **Annulation des bases de l'application**). Réalisez les actions suivantes dans la fenêtre **Planification** (cf. ill. 128) :

   a) Pour activer la planification, cochez la case **Exécuter de manière planifiée** ;

   b) Précisez la fréquence d'exécution de la tâche (cf. point B.2.1, p. 392) : choisissez une des options suivantes dans la liste **Fréquence** : **Chaque heure**, **Chaque jour**, **Chaque semaine**, **Au lancement de l'application**, **A l'actualisation des bases** (dans les tâches **Mise à jour des bases de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**, vous pouvez également indiquer la fréquence de lancement **Après réception des mises à jour par le serveur d'administration**) :

      - Si vous avez sélectionné **Chaque heure**, indiquez le nombre d'heures dans le champ **Chaque <chiffres> heures** du groupe de paramètres **Configuration du démarrage des tâches** ;
      - Si vous avez sélectionné **Chaque jour**, indiquez le nombre de jours dans le champ **Chaque <chiffres> jours** du groupe de paramètres **Configuration du démarrage des tâches** ;

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

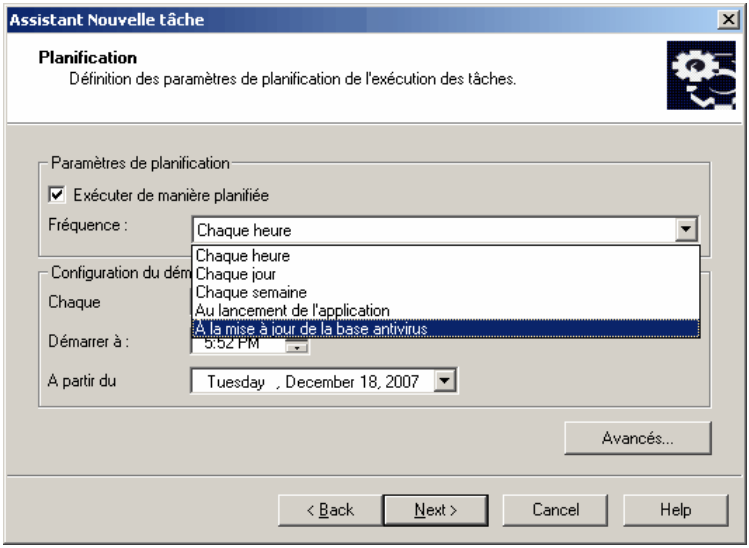

Illustration 128. Exemple de la fenêtre **Planification**, avec une fréquence configurée sur **À la mise à jour de la base antivirus**

c) Dans le champ **Démarrer à**, indiquez l'heure de la première exécution de la tâche ;dans le champ **A partir du**, indiquez la date d'entrée en vigueur de la planification. (cf. point B.2.2, p. 393) ;

d) Le cas échéant, définissez les autres paramètres de la planification : cliquez sur le bouton **Avancés** et dans la boîte de dialogue **Paramètres de planification avancés** (cf. ill. 129), exécutez les actions suivantes :

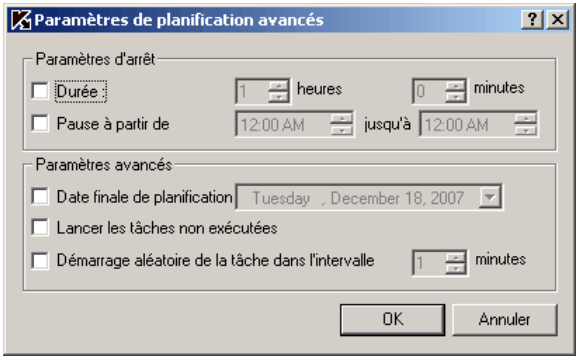

Illustration 129. Boîte de dialogue **Paramètres de planification avancés**

- Indiquez la durée maximale d'exécution de la tâche : dans le champ **Durée** du groupe **Paramètres d'arrêt**, saisissez les heures et les minutes souhaitées (cf. point B.2.4, p. 395) ;
- Définissez les plages horaires de la journée au cours desquelles l'exécution de la tâche sera suspendue : dans le groupe **Paramètres d'arrêt**, saisissez le début et la fin de l'intervalle dans le champ **Pause à partir de … jusqu'à** (cf. point B.2.5, p. 396) ;
- Indiquez la date à partir de laquelle la programmation ne sera plus en vigueur : cochez la case **Date finale de planification** et à l'aide de la boîte de dialogue **Calendrier**, sélectionnez la date à partir de laquelle la planification ne sera plus en vigueur (cf. point B.2.3, p. 394) ;
- Activez l'exécution des tâches non exécutées : cochez la case **Lancer les tâches non exécutées** (cf. point B.2.6, p. 396) ;
- Activez l'utilisation du paramètre **Répartition du lancement** : cochez la case **Démarrage aléatoire de la tâche dans l'intervalle** et saisissez la valeur du paramètre en minutes (cf. point B.2.7, p. 397).

e) Cliquez sur **OK**.

6. Si la tâche créée est une tâche globale, sélectionnez les ordinateurs du réseau (groupe) où elle sera exécutée.
7. Dans la fenêtre **Fin du travail** de l'Assistant de création de tâche, cliquez sur le bouton **Terminer**.

La tâche créée figure dans la boîte de dialogue **Tâches**.

21.3. Configuration de la tâche

Après avoir créé la tâche, vous pouvez la configurer de la manière suivante :

- Modifier les paramètres de la tâche ;
- Configurer/modifier la planification de la tâche ;
- Indiquer le compte utilisateur sous lequel la tâche sera exécutée ;
- Configurer les notifications sur les résultats de l'exécution des tâches.

Pour configurer une tâche :

1. Dans l'arborescence de la console d'administration, déployez le noeud **Groupes** puis, sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau des résultats, ouvrez le menu contextuel de la ligne contenant les informations relatives au serveur protégé puis, sélectionnez **Propriétés**.
3. Ouvrez le menu contextuel de la tâche que vous souhaitez configurer sur l'onglet **Tâches** de la fenêtre **Propriétés de l'ordinateur** puis, sélectionnez **Paramètres**.
4. Le cas échéant, modifiez les paramètres de la tâche :
   - Dans la tâche **Protection en temps réel des fichiers** sous l'onglet **Configuration** :

     Composez la zone de protection (pour en savoir plus sur les secteurs prédéfinis, consultez le point. 6.2.1.2 à la page 73).

     Appliquez la zone de confiance : cliquez sur le bouton **Mode de protection** et dans la boîte de dialogue **Avancé**, cochez la case **Appliquer la zone de confiance** (pour savoir comment constituer une zone de confiance, consultez le point 20.7.3 à la page 329) ;

     Modifiez le mode de protection des objets : cliquez sur le bouton **Mode de protection** et dans la boîte de dialogue **Avancé**, sélectionnez le mode de protection des objets requis (pour en savoir plus sur le paramètre, consultez le point B.3.1 à la page 399) ;
   - Dans la tâche **Analyse des scripts** sous l'onglet **Configuration** :

     Décidez s'il faut autoriser ou interdire l'exécution des scripts que Kaspersky Anti-Virus considère suspect ;

Appliquez la zone de confiance (pour savoir comment former une zone de confiance, consultez le point 20.7.3 à la page 329) ;

- Dans la tâche **Analyse complète** de l'ordinateur, sous l'onget **Couverture d'analyse** :

  Composez la couverture d'analyse (pour en savoir plus sur les couvertures prédéfinies, consultez le point 9.2.1.2 à la page 125) ;

  Modifiez la priorité du processus dans lequel la tâche sera exécutée (cf. point 9.3 à la page 145) ;

  Attribuez à la tâche l'état «Tâche d'analyse complete de l'ordinateur» (cf. point 21.4 , p. 347).

  Appliquez la zone de confiance (pour voir comment créer la zone de confiance, consultez le point 20.7.3 à la page 329) ;

- Dans la tâche **Copie des mises à jour** :

  Sous l'onglet **Configuration de la copie des mises à jour** indiquez la composition de la mise à jour et le répertoire de sauvegarde (cf. point B.5.7 à la page 432) ;

  Sous l'onglet **Source des mises à jour**, désignez la source des mises à jour (cf. ill. B.5.1 à la page 423) ;

- L'onglet **Planification** vous permet de programmer la tâche (cf. point 5 sur les instructions relatives à la création d'une tâche à la page 342) ;
- Sur l'onglet **Compte utilisateur**, indiquez le compte utilisateur sous lequel la tâche sera exécutée (cf. point 5.9.1, p. 65) ;
- Sur l'onglet **Notification**, configurez les notifications sur les résultats de l'exécution des tâches (pour en savoir plus, consultez le document *Kaspersky Administration Kit. Manuel de l'utilisateur*).

> **Remarque**
>
> Pendant l'application de la stratégie de Kaspersky Administration Kit, les valeurs des paramètres accompagnés dans la stratégie de l'icône 🔒 dans la boîte de dialogue **Propriétés de la tâche** de la console d'administration ne peuvent être modifiés.

5. Cliquez sur **OK**.
6. Cliquez sur le bouton **OK** dans la boîte de dialogue **Paramètres de la tâche** afin d'enregistrer les modifications.

21.4. Administration de l'analyse complète des serveurs Octroi du statut *Tâche d'analyse complète de l'ordinateur* à la tâche d'analyse à la demande

Par défaut, Kaspersky Administration Kit attribue l'état *Avertissement* au serveur si la tâche **Analyse complète de l'ordinateur** est réalisée moins souvent que le paramètre **Seuil de déclenchement de l'événement *L'analyse complète du serveur n'a pas été réalisée depuis longtemps***.

Vous pouvez administrer l'analyse complète de tous les serveurs faisant partie d'un groupe d'administration de la manière suivante :

1. Créez une tâche de groupe d'analyse à la demande. Dans la boîte de dialogue **Paramètres** de l'Assistant de création de tâches, sélectionnez l'état « Tâche d'analyse complète de l'ordinateur ». Les paramètres que vous avez défini (couverture d'analyse et paramètres de sécurité) seront les mêmes pour tous les serveurs du groupe. Programmez l'exécution de la tâche. Pour en savoir plus sur la création d'une tâche, consultez le point 21.2 à la page 335.

   Remarque

   Vous pouvez attribuer l'état « tâche d'analyse complète de l'ordinateur » au moment de la création de la tâche ou plus tard dans la boîte de dialogue **Paramètres de la tâche**.

2. A l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez la tâche prédéfinie **Analyse complète de l'ordinateur** sur les serveurs du groupe (cf. point 19.4, p. 299).

Dès ce moment, le serveur d'administration de Kaspersky Administration Kit évaluera l'état de la sécurité du serveur protégé et vous le signalera en fonction des résultats de la dernière exécution de la tâche dont l'état est « Tâche d'analyse complète de l'ordinateur » et non pas selon les résultats de l'exéctuion de la tâche prédéfinie **Analyse complète de l'ordinateur**.

Vous pouvez attribuer l'état « Tâche d'analyse complète de l'ordinateur » non seulement aux tâches de groupe, mais également aux tâches globales d'analyse à la demande.

La console de Kaspersky Anti-Virus dans MMC vous permet de voir si la tâche de groupe ou globale d'analyse à la demande est une tâche d'analyse complète de l'ordinateur.

Remarque

Dans la console de Kaspersky Anti-Virus, la case **Considérer comme une tâche d'analyse complète** apparaît dans les propriétés mais elle ne peut être modifiée.

PARTIE 4. COMPTEURS DE KASPERSKY ANTI-VIRUS

Cette section aborde les sujets suivants :

- Description des compteurs de performance pour l'application « System Monitor » (cf. Chapitre 22, p. 350) ;
- Description des compteurs et des pièges SNMP de Kaspersky Anti-Virus (cf. Chapitre 23, p. 360).

CHAPITRE 22. COMPTEUR DE PERFORMANCE POUR L'APPLICATION « SYSTEM MONITOR »

Ce chapitre contient les informations générales sur les compteurs de performance de Kaspersky Anti-Virus (cf. point 22.1, p. 350) et une description de chacun d'entre eux :

- Nombre total de requêtes rejetées (cf. point 22.2, p. 351) ;
- Nombre total de requêtes ignorées (cf. point 22.3, p. 352) ;
- Nombre de requêtes non traitées suite à un manque de ressources système (cf. point 22.4, p. 353) ;
- Nombre de requêtes envoyées pour traitement (cf. point 22.5, p. 354) ;
- Nombre moyen de flux du gestionnaire d'interception de fichiers (cf. point 22.6, p. 355) ;
- Nombre maximum de flux du gestionnaire d'interception de fichiers (cf. point 22.7, p. 356) ;
- Nombre d'objets infectés dans la file de traitement (cf. point 22.8, p. 356) ;
- Nombre d'objets traités par seconde (cf. point 22.9, p. 358).

22.1. Présentation des compteurs de performances de Kaspersky Anti-Virus

Si le composant **Compteurs de performances** est repris dans les composants installés de Kaspersky Anti-Virus, alors Kaspersky Anti-Virus enregistre ses compteurs de performance pendant l'installation pour l'application « System Monitor » de Microsoft Windows.

Grâce aux compteurs de Kaspersky Anti-Virus, vous pouvez contrôler les performances de Kaspersky Anti-Virus durant l'exécution des tâches de protection en temps réel. Vous pouvez identifier les goulots d'étranglement en cas d'utilisation avec d'autres applications et les manques de ressources. Vous pouvez diagnostiquer une mauvaise configuration de Kaspersky Anti-Virus et les échecs de fonctionnement.

Pour consulter les compteurs de performances de Kaspersky Anti-Virus, ouvrez la console **Performance** dans l'élément **Administration** du panneau de configuration.

Les points suivants abordent la définition des compteurs, les intervalles de calcul des relevés recommandés, les valeurs limites et les recommandations pour la configuration de Kaspersky Anti-Virus lorsque les compteurs dépassent ces valeurs.

22.2. Total de requêtes rejetées

Nom	Total de requêtes rejetées (Number of requests denied)
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de Kaspersky Anti-Virus , le calcul est réalisé depuis la dernière exécution de Kaspersky Anti-Virus. Kaspersky Anti-Virus ignore les objets dont les requêtes de traitement sont rejetées par les processus de travail de Kaspersky Anti-Virus.
Fonction	Ce compteur permet d'identifier : • La réduction de la qualité de la protection en temps réel en raison d'une charge complète des processus de Kaspersky Anti-Virus ; • L'interruption de la protection en temps réel en raison d'un refus du gestionnaire d'intercepteurs de fichiers.
Valeur normal / limite	0 / 1
Intervalle de calcul des relevés recommandés	1 heure

Recommandation pour la configuration si la valeur dépasse la valeur limite	Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés. Les situations suivantes sont envisageables en fonction du « comportement » du compteur : • Le compteur indique quelques processus rejetés durant une longue période : tous les processus de Kaspersky Anti-Virus étaient totalement occupés, si bien que Kaspersky Anti-Virus n'a pas pu analyser les objets. Pour éviter que des objets soient ignorés, augmentez le nombre de processus de Kaspersky Anti-Virus pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres **Nombre maximum de processus de travail actifs** (pour de plus amples informations sur ce paramètre, consultez le point B.1.1 à la page 377) et **Nombre de processus de travail actifs pour les tâches de protection en temps réel** (pour de plus amples informations, consultez le point B.1.2 à la page 378) de Kaspersky Anti-Virus ; • Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : le gestionnaire d'intercepteurs de fichiers ne fonctionne plus. Kaspersky Anti-Virus n'analyse plus les objets. Relancez Kaspersky Anti-Virus.

22.3. Total de requêtes ignorées

Nom	Total de requêtes ignorées (Number of requests skipped)
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par les processus du pilote mais qui n'ont pas donné d'événement sur la fin du traitement , le calcul est réalisé depuis la dernière exécution de Kaspersky Anti-Virus. Si la requête de traitement d'un objet reçue par un des processus de travail n'a pas envoyé d'événement sur la fin du traitement, le pilote transmet cette requête à un autre processus et la valeur du compteur **Total des requêtes ignorées** augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a accepté la requête de traitement (ils étaient occupés) ou n'a pas envoyé d'événement sur la fin du traitement, Kaspersky Anti-Virus

	ignore cet objet et la valeur du compteur **Total des requêtes rejetées** augmente d'une unité.
Fonction	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
Valeur normal / limite	0 / 1
Intervalle de calcul des relevés recommandés	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur diffère de zéro, cela signifie qu'un ou plusieurs flux du gestionnaire d'intercepteurs de fichiers sont gelés. La valeur du compteur correspond au nombre de flux gelés en ce moment. Si la vitesse d'analyse n'est pas satisfaisante, relancez Kaspersky Anti-Virus afin de rétablir les flux gelés.

22.4. Nombre de requêtes non traitées en raison d'un manque de ressources système

Nom	Nombre de requêtes non traitées en raison d'un manque de ressources (Number of requests not processed due to lack of ressources)
Définition	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Anti-Virus. Kaspersky Anti-Virus ignore les objets dont les requêtes de traitement ne sont pas traitées par le pilote d'interception de fichiers.
Fonction	Le compteur permet de repérer et de résoudre une éventuelle baisse de la qualité de la protection en temps réel provoquée par un manque de ressources.

Valeur normal / limite	0 / 1
Intervalle de calcul des relevés recommandés	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si le compteur affiche une valeur différente de zéro, les processus de travail de Kaspersky Anti-Virus ont besoin de plus de mémoire vive pour traiter les requêtes. Il se peut que les processus actifs d'autres applications utilisent toute la mémoire vive disponible.

22.5. Nombre de requêtes envoyées pour traitement

Nom	Nombre de requêtes envoyées pour traitement (Number of requests sent to be processed)
Définition	Nombre d'objets attendant d'être traités par les processus actifs de Kaspersky Anti-Virus en ce moment
Fonction	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Anti-Virus et le niveau général de l'activité de fichiers sur le serveur
Valeur normal / limite	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur le serveur
Intervalle de calcul des relevés recommandés	1 minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	non

22.6. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers (Average number of file interception dispatcher streams)
Définition	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (moyenne pour tous les processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une éventuelle détérioration de la qualité de la protection en temps réel en raison de la charge des processus de Kaspersky Anti-Virus et d'y remédier
Valeur normal / limite	Varie/40
Intervalle de calcul des relevés recommandés	1 minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Chaque processus actif peut accepter un maximum de 60 flux du gestionnaire d'intercepteurs de fichiers. Si la valeur du compteur approche de 60, il se peut qu'aucun des processus actifs ne puisse accepter une nouvelle requête de traitement du pilote d'intercepteurs de fichiers et Kaspersky Anti-Virus ignorera l'objet. Augmentez le nombre de processus de Kaspersky Anti-Virus pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres **Nombre maximum de processus de travail actifs** (pour de plus amples informations sur ce paramètre, consultez le point B.1.1 à la page 377) et **Nombre de processus de travail actifs pour les tâches de protection en temps réel** (pour de plus amples informations, consultez le point B.1.2 à la page 378) de Kaspersky Anti-Virus.

22.7. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers (Maximum number of file interception dispatcher streams)
Définition	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (nombre le plus élevé de processus impliqués dans les tâches de protection en temps réel à ce moment)
Fonction	Ce compteur permet d'identifier une réduction des performances en raison d'une répartition inégale de la charge dans les processus actifs exécutés et d'y remédier
Valeur normal / limite	Varie/40
Intervalle de calcul des relevés recommandés	1 minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur de ce compteur dépasse en permanence et de beaucoup la valeur du compte **Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers**, Kaspersky Anti-Virus répartit de manière inégale la charge sur les processus exécutés. Relancez Kaspersky Anti-Virus.

22.8. Nombre d'objets infectés dans la file de traitement

Nom	Nombre d'objets infectés dans la file de traitement (Number of items in the infecte object queue)

Définition	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment
Fonction	Ce compteur permet d'identifier : • L'interruption de la protection en temps réel en raison d'un éventuel refus du gestionnaire d'intercepteurs de fichiers. • La surcharge du processus suite à une répartition inégale du temps de processus entre Kaspersky Anti-Virus et les autres applications exécutées. • Les épidémies de virus.
Valeur normal / limite	La valeur du compteur peut être différente de zéro tandis que Kaspersky Anti-Virus traite les objets suspects ou infectés découverts mais elle revient sur zéro peu de temps après la fin du traitement / la valeur du compteur est différente de zéro pendant une longe période
Intervalle de calcul des relevés recommandés	Une minute

Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur n'est pas égale à zéro pendant une longue période : • Kaspersky Anti-Virus ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Relancez Kaspersky Anti-Virus. • Manque de temps de processus pour le traitement des objets ; Accordez à Kaspersky Anti-Virus plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur. • Une épidémie de virus s'est déclenchée. Vous pouvez activer la fonction Prévention des épidémies virales (cf. point 7.5, p. 102). L'émergence d'une épidémie de virus est également indiquée par le nombre d'objets infectés ou suspects découverts dans la tâche **Protection en temps réel des fichiers**. Vous pouvez consulter les informations relatives au nombre d'objets découverts dans les statistiques de la tâche (cf. point 6.2.3, p. 91) ou dans le rapport détaillé sur l'exécution de la tâche (cf. point 13.2.4, p. 211).

22.9. Nombre d'objets traités par seconde

Nom	Nombre d'objets traités par seconde (Number of objects processed per second)
Définition	Nombre d'objets traités par unité de temps pendant laquelle ces objets ont été traités ; le décompte s'opère sur des intervalles de temps égaux
Fonction	Ce compteur affiche la vitesse de traitement des objets ; il permet d'identifier une baisse des performances du serveur en raison d'un manque de temps de processus actif pour les processus de Kaspersky Anti-Virus ou d'un échec de Kaspersky Anti-Virus et d'y remédier

Valeur normal / limite	Varie / non
Intervalle de calcul des relevés recommandés	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Les valeurs du compteur dépendent des paramètres de Kaspersky Anti-Virus et de la charge des processus des autres applications sur le serveur. Observez le niveau moyen du compteur au cours d'une longue période. Si le niveau moyen baisse : • Les processus de travail de Kaspersky Anti-Virus ne disposent pas des ressources de processus suffisantes pour traiter les objets ; Accordez à Kaspersky Anti-Virus plus de temps de processus, par exemple en réduisant la charge des autres applications sur le serveur. • Un échec s'est produit dans le fonctionnement de Kaspersky Anti-Virus (plusieurs flux sont gelés). Relancez Kaspersky Anti-Virus.

CHAPITRE 23. COMPTEURS ET PIEGES SNMP DE KASPERSKY ANTI-VIRUS

Le présent chapitre aborde les sujets suivants :

- Présentation des compteurs et des pièges SNMP de Kaspersky Anti-Virus (cf. point 23.1, p. 360) ;
- Description des compteurs SNMP (cf. point 23.2, p. 360) ;
- Description des pièges SNMP (cf. point 23.2.8, p. 365).

23.1. Présentation des compteurs et pièges SNMP de Kaspersky Anti-Virus

Si vous avez inclus le composant **Compteurs et pièges SNMP** dans les composants de Kaspersky Anti-Virus à installer, vous pouvez consulter les compteurs et les pièges de Kaspersky Anti-Virus selon les protocoles Simple Network Management Protocol (SNMP) et HP Open View.

Pour consulter les compteurs et les pièges de Kaspersky Anti-Virus depuis l'ordinateur-poste de travail de l'administrateur, lancez sur le serveur protégé le service SNMP (SNMP Service) et le service de pièges SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

23.2. Compteurs SNMP de Kaspersky Anti-Virus

Kaspersky Anti-Virus prévoit les compteurs SNMP suivants :

- Compteurs de performances (cf. point 23.2.1, p. 361) ;
- Compteurs généraux (cf. point 23.2.2, p. 361) ;

- Compteur de mise à jour (cf. point 23.2.3, p. 362) ;
- Compteurs de protection en temps réel (cf. point 23.2.4, p. 362) ;
- Compteurs de quarantaine (cf. point 23.2.5, p. 364) ;
- Compteurs de sauvegarde (cf. point 23.2.6, p. 364) ;
- Compteurs d'interdiction de l'accès des ordinateurs au serveur (cf. point 23.2.7, p. 364).
- Compteurs d'analyse des scripts (cf. point 23.2.8, p. 365)

23.2.1. Compteurs de performances

Compteur	Définition
currentRequestsAmount	Nombre de requêtes envoyées pour traitement (cf. description au point 22.5, p. 354)
currentInfectedQueueLength	Nombre d'objets infectés dans la file de traitement (cf. description au point 22.8, p. 356)
currentObjectProcessingRate	Nombre d'objets traités par seconde (cf. description au point 22.9, p. 358)
currentWorkProcessesAmount	Nombre de processus de travail de Kaspersky Anti-Virus en ce moment

23.2.2. Compteurs généraux

Compteur	Définition
currentApplicationUptime	Durée de fonctionnement de Kaspersky Anti-Virus depuis sa dernière exécution (en centièmes de secondes)
currentFileMonitorTaskStatus	Etat de la tâche **Protection en temps réel des fichiers** : On : en cours ; Off : arrêtée ou suspendue
currentScriptCheckerTaskStatus	Etat de la tâche **Analyse des scripts** : On : en cours ; Off : arrêtée ou suspendue

Compteur	Définition
lastFullScanAge	« Age » de la dernière analyse complète du serveur (intervalle de temps en secondes entre la date de fin de la tâche portant le statut *tâche d'analyse complète de l'ordinateur* et le moment actuel)
licenseExpirationDate	Date de fin de validité de la clé (Si une clé de licence et une clé de réserve sont installées, alors cette donnée indique la fin de validité de synthèse des clés active et de synthèse)

23.2.3. Compteur de mise à jour

Compteur	Définition
avBasesAge	« Age des bases » (intervalle de temps en centième de seconde entre la date de création des dernières mises à jour installée et l'heure actuelle)

23.2.4. Compteurs de protection en temps réel

Compteur	Définition
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalInfectedObjectsFound	Nombre d'objets infectés découverts depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalSuspiciousObjectsFound	Nombre d'objets suspects découverts depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**

Compteur	Définition
totalVirusesFound	Nombre de menaces découvertes depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsQuarantined	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotQuarantined	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsDisinfected	Nombre total d'objets infectés réparés par Kaspersky Anti-Virus ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotDisinfected	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus a tenté de réparer en vain ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsDeleted	Nombre total d'objets infectés ou suspects, que Kaspersky Anti-Virus a supprimé ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsNotDeleted	Nombre total d'objets infectés ou suspects que Kaspersky Anti-Virus aurait dû supprimer ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**
totalObjectsBackedUp	Nombre total d'objets infectés que Kaspersky Anti-Virus a placé en sauvegarde ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**

Compteur	Définition
totalObjectsNotBackedUp	Nombre total d'objets infectés que Kaspersky Anti-Virus a tenté de placer en vain en sauvegarde ; ce nombre est calculé depuis la dernière exécution de la tâche **Protection en temps réel des fichiers**

23.2.5. Compteurs de quarantaine

Compteur	Définition
totalObjects	Nombre d'objets présents actuellement en quarantaine
totalSuspiciousObjects	Nombre d'objets suspects présents actuellement en quarantaine
currentStorageSize	Volume de données en quarantaine (Mo)

23.2.6. Compteurs de sauvegarde

Compteur	Définition
currentBackupStorageSize	Volume de données en sauvegarde (Mo)

23.2.7. Compteurs d'interdiction d'accès des ordinateurs au serveur

Compteur	Définition
currentHostsBlocked	Nombre d'ordinateurs interdits dans la liste
totalNotBlocked	Nombre d'opérations d'interdiction d'accès des ordinateurs non exécutées en tant qu'exclusion du blocage (ordinateurs de confiance) depuis l'activation de la fonction d'interdiction automatique

23.2.8. Compteurs d'analyse des scripts

Compteur	Description
totalScriptsProcessed	Total de scripts analysés
totalInfectedIDangerous-ScriptsFound	Total des scripts infectés découverts
totalSuspiciousScriptsFound	Total des scripts suspects découverts
totalScriptsBlocked	Total des scripts dont l'accès a été bloqué

23.3. Pièges SNMP

Le tableau suivant décrit les pièges SNMP de Kaspersky Anti-Virus ; les paramètres des pièges sont décrits au tableau dessous.

Piège	Description	Paramètres
eventThreatDetected	Menace détectée. Pour en savoir plus sur la façon dont Kaspersky Anti-Virus découvre les objets infectés et suspects, lisez le point 1.1.3 à la page 20.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSi-zeExceeds	Dépassement de la taille maximum de sauvegarde. Le volume total de données de la sauvegarde dépasse la valeur du paramètre **Taille maximale de la sauvegarde**. Kaspersky Anti-Virus continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource

Piège	Description	Paramètres
EventThresholdBackup StorageSizeExceeds	Le seuil d'espace libre pour la sauvegarde est atteint. La quantité d'espace libre dans la sauvegarde, définie par le paramètre **Seuil d'espace libre de la sauvegarde**, est revenue à la valeur indiquée. Kaspersky Anti-Virus continue à mettre les objets infectés en sauvegarde.	eventDateAndTime eventSeverity eventSource
EventQuarantineStorage SizeExceeds	Dépassement de la taille maximum de quarantaine. Le volume total de données de la quarantaine dépasse la valeur du paramètre **Taille maximale de la quarantaine**. Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Le seuil d'espace libre pour la quarantaine est atteint. La quantité d'espace libre dans la quarantaine, définie par le paramètre **Seuil d'espace libre de la quarantaine**, est revenue à la valeur indiquée. Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine.	eventDateAndTime eventSeverity eventSource
EventObjectNot Quarantined	Erreur de placement de l'objet en quarantaine	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason

Piège	Description	Paramètres
eventObjectNotBackuped	Erreur de conservation d'une copie de l'objet en sauvegarde	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
EventQuarantineInternal Error	Une erreur de quarantaine s'est produite	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Une erreur de sauvegarde s'est produite	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	La base de donnée n'est plus à jour. Le nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des base (tâche locale, de groupe ou globale)	eventSeverity eventDateAndTime eventSource days
EventAVBasesTotally Outdated	La base de données est périmée. Le nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des base (tâche locale, de groupe ou globale)	eventSeverity eventDateAndTime eventSource days
EventApplicationModules IntegrityFailed	Une erreur s'est produite durant l'analyse de l'intégrité des modules de l'application	eventSeverity eventDateAndTime eventSource

Piège	Description	Paramètres
eventApplicationStarted	Kaspersky Anti-Virus est lancé	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Anti-Virus est arrêté.	eventSeverity eventDateAndTime eventSource
EventFullScanWasnt PerformForALongTime	La dernière analyse complète de votre ordinateur a été réalisée il y a longtemps. Le nombre de jour écoulé depuis la dernière tâche dont le statut est *Tâche d'analyse complète de l'ordinateur* est compté	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	La durée de validité de la clé est écoulée	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	La clé de licence arrive bientôt à échéance. Le nombre de jour restant avant la fin de la validité de la clé est compté	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Erreur d'exécution de la tâche	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName

Piège	Description	Paramètres
eventUpdateError	Erreur d'exécution de la tâche de mise à jour	eventSeverity eventDateAndTime taskName updaterErrorEventReason

Le tableau suivant décrit les paramètres des pièges et valeurs possibles.

Paramètre	Description et valeurs possibles
eventDateAndTime	Heure à laquelle l'événement est survenu
eventSeverity	Degré d'importance de l'événement. Valeurs possibles : • critical (1) – critique, • warning (2) – avertissement, • info (3)– informations
UserName	Nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté)
computerName	Nom de l'ordinateur (par exemple, nom de l'ordinateur dont l'utilisateur a tenté d'accéder à un fichier infecté)

Paramètre	Description et valeurs possibles
eventSource	Source de l'événement : Composant fonctionnel pendant le fonctionnement duquel l'événement s'est produit. Valeurs possibles : • unknown (0) – composant fonctionnel non identifié ; • quarantine (1) – Quarantaine ; • backup (2) – Sauvegarde ; • reporting (3) – Rapports ; • updates (4)– Mise à jour ; • realTimeProtection (5) –Protection en temps réel ; • onDemandScanning (6) – Analyse à la demande ; • product (7) – événement lié non pas au fonctionnement d'un composant particulier mais au fonctionnement de Kaspersky Anti-Virus dans son ensemble ; • systemAudit (8) – Journal d'audit système ; • hostBlocker(9) – Interdiction d'accès des ordinateurs au serveur.
eventReason	Cause de l'événement. Valeurs possibles : • reasonUnknown (0) – cause indéterminée, • reasonInvalidSettings (1) – uniquement pour les événements de la sauvegarde et de la quarantaine, s'affiche si le dossier de sauvegarde ou de quarantaine est inaccessible (privilèges d'accès insuffisants ou le chemin de réseau indiqué dans les paramètres de la quarantaine est incorrect). Dans ce cas, Kaspersky Anti-Virus utilisera le dossier de sauvegarde ou de quarantaine indiqué par défaut.
objectName	Nom de l'objet (par exemple, nom du fichier contenant la menace)
threatName	Nom de menace

Paramètre	Description et valeurs possibles
detectType	Type de menace. Valeurs possibles : • undefined (0) – indéterminée ; • virware – virus et vers de réseau traditionnels ; • trojware – chevaux de Troie ; • malware – autres programmes malveillants ; • adware – logiciels publicitaires ; • pornware – programmes au contenu pornographiques ; • riskware – applications présentant un risque potentiel. Pour obtenir de plus amples informations sur les types de menace, lisez le 1.1.2 à la page 16.
detectCertainty	Degré de certitude de la découverte d'une menace. Valeurs possibles : • Warning (avertissement) L'analyseur heuristique considère cet objet comme un objet suspect ; • Suspicion (suspect). L'objet est suspect ; il existe une équivalence partielle entre une partie du code de l'objet et une partie du code d'une menace connue ; • Sure (infecté). L'objet est infecté ; il existe une équivalence parfaite entre une partie du code de l'objet et une partie du code d'une menace connue.
days	Nombre de jours (par exemple, nombre de jours d'ici la fin de validité de la clé)
errorCode	Code erreur
knowledgeBaseId	Adresse de l'article dans la banque de solutions (par exemple, adresse de l'article décrivant une erreur quelconque)
taskName	Nom de tâche

Paramètre	Description et valeurs possibles
updaterErrorEventReason	Cause de la non application des mises à jour. Les valerus possibles sont : • reasonUnknown(0) – erreur inconnue ; • reasonAccessDenied – accès interdit ; • reasonUrlsExhausted – fin de la liste des sources de mise à jour ; • reasonInvalidConfig – fichier de configuration incorrect ; • reasonInvalidSignature – signature invalide ; • reasonCantCreateFolder – creation du repertoire impossible ; • reasonFileOperError – erreur de fichier ; • reasonDataCorrupted – objet corrompu ; • reasonConnectionReset – arrêt de la connexion ; • reasonTimeOut – délai d'attente pour la connexion expiré ; • reasonProxyAuthError – erreur de verification de l'authenticité sur le serveur proxy ; • reasonServerAuthError – erreur de verification de l'authenticité sur le serveur ; • reasonHostNotFound – ordinateur introuvable ; • reasonServerBusy – serveur inaccessible ; • reasonConnectionError – erreur de connexion ; • reasonModuleNotFound – objet introuvable ; • reasonBlstCheckFailed(16) – erreur de verification de la liste des licences rappelées. Il se peut qu'une actualisation ait été diffusée au moment de la mise à jour des base. Il faudra retenter la mise à jour après quelques minutes. Consultez la description de ces causes et les actions que l'administrateur du site peut entreprendre sur le site de service d'assistance technique.

Paramètre	Description et valeurs possibles
StorageObjectNot AddedEventReason	Cause du non placement de l'objet en sauvegarde ou en quarantaine. Les valeurs possibles sont : • reasonUnknown(0) – raison inconnue ; • reasonStorageInternalError – erreur dans les bases de données ; restaurez Kaspersky Anti-Virus ; • reasonStorageReadOnly – la base de données est uniquement accessible en lecture ; restaurez Kaspersky Anti-Virus ; • reasonStorageIOError – erreur d'entrée/de sortie : a) Kaspersky Anti-Virus est corrompu, restaurez-le ; b) le disque sur lequel les fichiers de Kaspersky Anti-Virus sont sauvegardés est abîmé ; • reasonStorageCorrupted – le referential est abîmé ; restaurez Kaspersky Anti-Virus ; • reasonStorageFull – la base de données est remplie ; faites de la place sur le disque ; • reasonStorageOpenError – échec de l'ouverture du fichier de base de données ; restaurez Kaspersky Anti-Virus ; • reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigencies de Kaspersky Anti-Virus ; • reasonObjectNotFound – l'objet place dans le référenciel n'existe pas sur le disque ; • reasonObjectAccessError – privileges insuffisants pour l'utilisation de Backup API: le compte utilisateur sous les privilèges duquel l'opération est réalisée ne jouit pas des privilèges Backup Operator ; • reasonDiskOutOfSpace – espace insuffisant sur le disque.

ANNEXE A. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé la solution à votre problème dans ce manuel ou dans la rubrique **Service / Banque de solutions** du site de Kaspersky Lab (www.kaspersky.fr), contactez le service d'assistance technique de Kaspersky Lab.

Remarque

Pour bénéficier du service d'Assistance technique, vous devez communiquer votre numéro de client et votre mot de passe à l'opérateur. Pour obtenir le numéro de client et le mot de passe, vous devez vous enregistrer sur le site du service d'assistance technique à l'adresse https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/?LANG=fr, en saisissant le numéro de série de clé.

Vous pouvez contactez les experts du service d'assistance technique de l'une des méthodes suivantes :

- Si le problème est urgent, composez le numéro de téléphone repris dans la section **Coordonnées** (cf. Point C.2, p. 456) de la présente documentation. L'assistance téléphonique est offerte en russe, en anglais, en français et en allemand, 24h/24.
- Vous pouvez poser des questions aux experts du service d'assistance technique via un formulaire en ligne spécial dans le système Helpdesk accessible à la page http://support.kaspersky.ru/helpdesk.html?LANG=fr. Les experts du service d'assistance technique répondront à vos questions par courrier électronique envoyé à l'adresse saisie dans le formulaire.

  Lorsque vous remplissez le formulaire, décrivez le plus exactement possible le problème. Dans les champs obligatoires, saisissez :

  - **Le type de requête**. Les questions que les utilisateurs posent le plus souvent sont regroupées en thèmes séparés, par exemple « Problème d'installation/de suppression du logiciel » ou « Problème de recherche/de neutralisation de virus ». Si vous ne trouvez pas le thème qui se rapporte à votre cas, choisissez « Question générale ».

- **Logiciel** : Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.
- **Le texte du message**. Décrivez le plus exactement possible votre problème.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement.
- **Courrier électronique**. Les experts du service d'assistance technique enverront leurs réponses à cette adresse.

ANNEXE B. DESCRIPTION DES PARAMETRES GENERAUX DE KASPERSK ANTI-VIRUS, DES PARAMETRES DE SES FONCTIONS ET DE SES TACHES

B.1. Paramètres généraux de Kaspersky Anti-Virus

Vous pouvez configurer les paramètres généraux suivants dans Kaspersky Anti-Virus :

- Nombre maximum de processus de travail (cf. point B.1.1, p. 377) ;
- Nombre maximum de processus pour la protection en temps réel (cf. point B.1.2, p. 378) ;
- Nombre de processus pour les tâches d'analyse à la demande en arrière-plan (cf. point B.1.3, p. 379) ;
- Restauration des tâches (cf. point B.1.4, p. 380) ;
- Durée de conservation des informations reprises dans le noeud **Rapports** (cf. point B.1.5, p. 381) ;
- Durée de conservation des informations reprises dans le noeud **Enregistrement d'audit système** (cf. point B.1.6, p. 382) ;
- Actions réalisées lors du passage à l'alimentation de la batterie (cf. B.1.7, p. 383) ;
- Seuil de déclenchement des événements (cf. point B.1.8, p. 383) ;
- Constitution d'un journal de traçage (cf. point B.1.9, p. 384) ;
- Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (cf. point B.1.10, p. 390).

B.1.1. Nombre maximum de processus de travail actifs

<table>
<tr><td>Paramètre</td><td>Nombre maximum de processus de travail actifs</td></tr>
<tr><td>Description</td><td>Ce paramètre appartient au groupe de paramètres Adaptabilité de Kaspersky Anti-Virus. Il définit le nombre maximum de processus de travail qui peuvent être exécutés simultanément par Kaspersky Anti-Virus.

Les processus de travail de Kaspersky Anti-Virus sont chargés de la protection en temps réel, de l'analyse à la demande et de la mise à jour.

L'augmentation du nombre de processus de travail exécutés en parallèle accélère la vitesse d'analyse des fichiers et la résistance de Kaspersky Anti-Virus aux échecs. Toutefois, si cette valeur est trop élevée, les performances globales du serveur peuvent chuter et la mémoire vive requise peut augmenter.

Remarque

N'oubliez pas que la console d'administration de l'application Kaspersky Administration Kit vous permet de définir le paramètre Nombre maximum de processus de travail actifs uniquement pour Kaspersky Anti-Virus sur un serveur distinct (dans la boîte de dialogue Paramètres de l'application) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.</td></tr>
<tr><td>Valeurs possibles</td><td>1– 8</td></tr>
<tr><td>Valeur par défaut</td><td>Kaspersky Anti-Virus réalise une montée en capacité automatique en fonction du nombre de processeur sur le serveur :

<table>
<tr><th>Nombre de processeurs</th><th>Nombre maximum de processus actifs</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>1< nbre de processeurs < 4</td><td>2</td></tr>
<tr><td>≥ 4</td><td>4</td></tr>
</table>
</td></tr>
</table>

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.2. Nombre de processus pour la protection en temps réel

Paramètre	Nombre de processus pour la protection en temps réel
Description	Ce paramètre appartient au groupe de paramètres **Adaptabilité** de Kaspersky Anti-Virus. Grâce à ce paramètre, vous pouvez définir un nombre fixe de processus qui serviront à Kaspersky Anti-Virus pour l'exécution de la protection en temps réel. La valeur plus élevée de ce paramètres accélère l'analyse des objets dans les tâches liées à la protection en temps réel. Toutefois, plus le nombre de processus de travail affectés à Kaspersky Anti-Virus est élevé, plus grand sera l'effet sur les performances globales du serveur protégé et sur son utilisation de la mémoire vive. **Remarque** N'oubliez pas que la console d'administration de l'application Kaspersky Administration Kit vous permet de définir le paramètre **Nombre de processus de protection en temps réel** uniquement pour Kaspersky Anti-Virus sur un serveur distinct (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe de serveurs.
Valeurs possibles	Valeurs possibles : 1-N, où N est la valeur définie par le paramètre **Nombre maximum de processus de travail actifs**. Si le **Nombre de processus de protection en temps réel** défini est égal au **Nombre maximum de processus de travail actifs**, vous diminuez l'impact de Kaspersky Anti-Virus sur la vitesse de l'échange de fichiers entre les postes et le serveur, tout en augmentant sa vitesse de réaction pendant la protection en temps réel. Toutefois, les tâches de mise à jour et les tâches d'analyse à la demande avec la priorité de base **Moyenne** (**Normal**) seront executes dans les processus de travail de Kaspersky Anti-Virus

<table>
<tr><td></td><td>déjà lances. Les tâches d'analyse à la demande seront exécutées plus lentement. Si l'exécution de la tâche entraîne un échec, son redémarrage prendra plus de temps.

Les tâches d'analyse à la demande avec une priorité de base Faible (Low) seront toujours exécutée dans un processus séparé ou dans des processus (cf. point B.1.3, p. 379).</td></tr>
<tr><td>Valeur par défaut</td><td>Kaspersky Anti-Virus réalise une montée en capacité automatique en fonction du nombre de processeur sur le serveur :
<table><tr><th>Nombre de processeurs</th><th>Nombre de processus pour la protection en temps réel</th></tr><tr><td>=1</td><td>1</td></tr><tr><td>> 1</td><td>2</td></tr></table></td></tr>
</table>

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.3. Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan

Paramètre	Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan
Description	Ce paramètre appartient au groupe de paramètres **Adaptabilité** de Kaspersky Anti-Virus. Grâce à ce paramètre, vous pouvez définir un nombre maximum de processus qui serviront à Kaspersky Anti-Virus pour l'exécution de l'analyse à la demande en arrière-plan. Le nombre de processus que vous définissez à l'aide de ce paramètre ne fait pas partie du total des processus de travail de Kaspersky Anti-Virus défini à l'aide du paramètre **Nombre maximum de processus actifs**. Par exemple, si vous procédez à la configuration suivante :

	• Nombre maximum de processus actifs – 3 ; • Nombre de processus pour les tâches de protection en temps réel – 3 ; • Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan – 1 ; et puis que vous lancez la tâche de protection en temps réel et une tâche d'analyse à la demande en arrière-plan, le nombre total de processus de travail de kavfswp.exe de Kaspersky Anti-Virus est de 4. Un processus de travail de faible priorité peut exécuter plusieurs tâches d'analyse à la demande. Vous pouvez augmenter le nombre de processus de travail, par exemple si vous lancez simultanément plusieurs tâches en arrière-plan, afin d'attribuer des processus distincts à chaque tâche. L'attribution de processus distincts aux tâches augmente la fiabilité de l'exécution de ces tâches .
Valeurs possibles	1-4
Valeur par défaut	1

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.4. Restauration des tâches

Paramètre	Restauration des tâches (**Ne pas réaliser la restauration des tâches d'analyse à la demande plus de … fois**)

Description	Ce paramètre appartient au groupe de paramètres **Fiabilité** de Kaspersky Anti-Virus. Il active la restauration des tâches lorsque celles-ci se solde par une erreur et définit le nombre de tentatives de restauration des tâches d'analyse à la demande. Lorsqu'une tâche se solde par un échec, le processus kavfs.exe de Kaspersky Anti-Virus tente de relancer le processus dans lequel cette tâche était exécutée au moment de l'arrêt. *Si la restauration des tâches est désactivée*, Kaspersky Anti-Virus ne restaure pas les tâches d'analyse à la demande et de protection en temps réel. *Si la restauration des tâches est activée*, Kaspersky Anti-Virus tente de restaurer les tâches de protection en temps réel jusqu'à la réussite de l'opération et tente de restaurer les tâches d'analyse à la demande autant de fois que le précise le paramètre.
Valeurs possibles	Activée / désactivée Nombre de tentatives de restauration des tâches d'analyse à la demande : 1-10
Valeur par défaut	La restauration des tâches est activée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 2

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.5. Durée de conservation des rapports

Paramètre	Durée de conservation des rapports (**Ne pas conserver les rapports et les événements plus de**)
Description	Ce paramètre définit le nombre de jours de conservation des rapports détaillés et de synthèse sur l'exécution des tâches affichés dans la console de Kaspersky Anti-Virus dans MMC dans le noeud **Rapports**. Vous pouvez désactiver ce paramètre afin de conserver indéfiniment les rapports sur l'exécution des tâches. Dans ce cas, la taille du fichier de rapport peut devenir très grande.

Valeurs possibles	1–365
Valeur par défaut	Les enregistrements relatifs aux événements survenus il y a plus de 30 jours sont supprimés des rapports détaillés sur l'exécution des tâches de Kaspersky Anti-Virus. Les rapports de synthèse sur les tâches exécutées sont supprimés 30 jours après la fin des tâches.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.6. Durée de conservation des événements dans le journal d'audit système

Paramètre	Durée de conservation du journal d'audit système (**Ne pas conserver les événements plus de … jours**)
Description	Vous pouvez limiter la durée de conservation des événements qui figurent dans le noeud **Enregistrement d'audit système** de la console Kaspersky Anti-Virus dans MMC
Valeurs possibles	1–365
Valeur par défaut	Les événements du journal d'audit système ne sont pas supprimés

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.7. Actions dans le fonctionnement sur la source d'alimentation de secours

Paramètre	Utilisation de la source d'alimentation de secours
Description	Ce paramètre définit les actions exécutées par Kaspersky Anti-Virus lorsque le serveur fonctionne sur l'alimentation électrique de secours.
Valeurs possibles	• Lancer/ne pas lancer les tâches d'analyse à la demande qui ont été programmées ; • Exécuter / arrêter toutes les tâches d'analyse à la demande lancées.
Valeur par défaut	Par défaut, lorsque le serveur tourne sur l'alimentation électrique d'urgence, Kaspersky Anti-Virus : • N'exécute pas les tâches d'analyse à la demande qui ont été programmées ; • Arrête automatiquement toutes les tâches d'analyse à la demande lancées.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.8. Seuil de déclenchement des événements

Paramètre	Seuil de déclenchement des événements

Description	Vous pouvez définir le seuil de déclenchement des événements des trois types suivants : • *La base de donnée est dépassée* et *La base de données est périmée*. Cet événement se déclenche lorsque les bases de Kaspersky Anti-Virus ne sont pas actualisées durant une période (nombre de jours) définie depuis la création des dernières mises à jour des bases. Vous pouvez configurer la notification de l'administrateur lorsque ces événements surviennent. • *L'analyse complète de l'ordinateur n'a pas été réalisée depuis longtemps*. Cet événement se déclenche si aucune des tâches accompagnées de la case **Considérer comme une tâche d'analyse complète de l'ordinateur** n'a été exécutée au cours du nombre de jours indiqués. Pour en savoir plus sur l'état « tâche d'analyse complète de l'ordinateur », consultez le point 21.4 à la page 347.
Valeurs possibles	Nombre de jours compris entre 1 et 365
Valeur par défaut	*La base de donnée n'est plus à jour* – 7 jours ; *La base de donnée est périmée* – 14 jours ; *L'analyse complète de l'ordinateur n'a pas été réalisée depuis longtemps* – 30 jours.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.9. Paramètres du journal de traçage

- Constitution d'un journal de traçage (cf. point B.1.9.1, p. 385) ;
- Répertoire contenant les fichiers du journal de traçage (cf. point B.1.9.2, p. 386) ;
- Niveau de détail du journal de traçage (cf. point B.1.9.3, p. 387) ;
- Taille d'un fichier du journal de traçage (cf. point B.1.9.4, p. 387) ;
- Traçage uniquement de certains sous-système de Kaspersky Anti-Virus (cf. point B.1.9.5, p. 388).

B.1.9.1. Constitution d'un journal de traçage

Paramètre	Constitution d'un journal de traçage (**Consigner les informations de débogage dans le fichier**)
Description	Le paramètre **Constitution d'un journal de traçage** appartient au groupe de paramètres **Interaction avec l'utilisateur**. Si un problème est survenu pendant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus ou une tâche en particulier s'est soldé par un échec ou ne se lance pas) et que vous souhaitez le diagnostiquer, vous pouvez créer un journal de traçage et envoyer les fichiers de ce journal au service d'assistance technique de Kaspersky Lab qui procédera à un examen. Pour obtenir de plus amples informations sur la manière de contacter le service d'assistance technique, consultez le point 1.2.3 à la page 24. Le journal de traçage de chaque processus de Kaspersky Anti-Virus est conservé dans un fichier distinct.

Valeurs et certaines recommandations quant à leur utilisation	Le journal de traçage est constitué/n'est pas constitué.
	Pour activer la constitution du fichier de traçage, il faut définir le répertoire dans lequel ces fichiers seront enregistrés.
	Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via une console installée sur un autre ordinateur, vous devrez indiquer les paramètres du journal de traçage dans la clé de registre suivante puis fermer et ouvrir à nouveau la console de Kaspersky Anti-Virus dans MMC afin d'activer la tenue du journal de traçage du sous-système **gui**.
	• Si une version 32 bits de Microsoft Windows est installée sur le serveur protégé :
	`HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE\6.0\Trace\Configuration=subsystem=gui;level=info;sink=folder(<répertoire pour les fichiers journaux et chemin d'accès>);roll=50000;layout=basic;logging=on`
	• Si une version 64 bits de Microsoft Windows est installée sur le serveur protégé :
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\Trace\Configuration=subsystem=gui;level=info;sink=folder(<répertoire pour les fichiers du journal de traçage et chemin d'accès>);roll=50000;layout=basic;logging=on`

Valeur par défaut	Le journal de traçage n'est pas constitué.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.9.2. Dossier contenant les fichiers du journal de traçage

Paramètre	Dossier contenant les fichiers du journal de traçage(**Dossier des fichiers de débogage**)
Description	Pour activer la constitution du fichier de traçage, il faut définir le répertoire dans lequel ces fichiers seront enregistrés
Valeurs et certaines recommandations quant à leur utilisation	Identifiez le répertoire sur le disque local du serveur protégé. Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Les répertoires de réseau ou les répertoires créés à l'aide de la commande SUBST ne peuvent faire office de répertoire pour l'enregistrement du fichier de traçage. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via MMC, installé sur le poste de travail distant de l'administrateur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur
Valeur par défaut	Non définie

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.9.3. Niveau de détail du journal de traçage

Paramètre	Niveau de détail du journal de traçage
Description	Vous pouvez sélectionner le niveau de détail du journal de traçage (*Informations de mise au point, Evénements d'information*, *Événements importants*, *Erreurs* ou *Événements critiques*)
Valeurs et certaines recommandations quant à leur utilisation	Le niveau le plus détaillé est le niveau *Informations de mise au point* où tous les événements sont consignés dans le journal tandis que le niveau le moins détaillé est le niveau *Événements critiques* où seuls les événements critiques sont consignés. N'oubliez pas que le journal de traçage peut prendre beaucoup de place sur le disque
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé sa constitution, Kaspersky Anti-Virus réalisera le traçage de tous les sous-systèmes de Kaspersky Anti-Virus au niveau de détails *Informaions de débogage*

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.1.9.4. Taille d'un fichier du journal de traçage

Paramètre	Taille d'un fichier du journal de traçage
Description	Vous pouvez modifier la taille maximale d'un fichier du journal
Valeurs et certaines recommandations quant à leur utilisation	1 à -999 Mo Dès que la taille du fichier de rapport atteint la valeur maximale, Kaspersky Anti-Virus consigne les informations dans un nouveau fichier ; le fichier journal antérieur est préservé
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé sa constitution, alors la taille maximale d'un fichier du journal sera de 50 Mo

B.1.9.5. Traçage de sous-systèmes individuels de Kaspersky Anti-Virus

Paramètre	Traçage de certains sous-systèmes uniquement de Kaspersky Anti-Virus
Description	Vous pouvez consigner dans le journal uniquement certains sous-systèmes de Kaspersky Anti-Virus si vous le souhaitez
Valeurs et certaines recommandations quant à leur utilisation	Dans la boîte de dialogue de configuration des paramètres de Kaspersky Anti-Virus, groupe de paramètres **Interaction avec l'utilisateur**, cliquez sur le bouton **Avancé** et dans la boîte de dialogue **Paramètres avancés**, champ **Composants de mise au point**, saisissez les codes des sous-systèmes pour lesquels vous souhaitez un traçage. Les codes des sous-systèmes doivent être séparés par une virgule. La saisie des codes est sensible à la case. Les codes et les noms des sous-systèmes de Kaspersky Anti-Virus sont repris dans le tableau 29. Les paramètres de traçage du sous-système gui (module enfichable de Kaspersky Anti-Virus) sont appliqués après le redémarrage de la console de Kaspersky Anti-Virus ; les paramètres de traçage du sous-système AK_conn (sous-système d'intégration à l'Agent d'administration de Kaspersky Administration Kit), après le redémarrage de l'agent d'administration de Kaspersky Administration Kit ; les paramètres de traçage des autres sous-systèmes de Kaspersky Anti-Virus sont appliqués directement après l'enregistrement des paramètres.
Valeur par défaut	Si vous ne modifiez pas les paramètres du journal de traçage après avoir activé sa constitution, Kaspersky Anti-Virus réalisera le traçage de tous les sous-systèmes de Kaspersky Anti-Virus

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

Le tableau suivant reprend la liste des codes des sous-systèmes de Kaspersky Anti-Virus dont les informations peuvent être ajoutées au fichier de traçage.

Tableau 29. Liste des codes des sous-systèmes pouvant être ajoutés au journal de traçage

Code de sous-système	**Nom du sous-système**
*	Tous les sous-systèmes (par défaut)
gui	Apparence de Kaspersky Anti-Virus dans MMC
AK_conn	Sous-système d'intégration à l'agent d'administration de Kaspersky Administration Kit
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Anti-Virus
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance de Kaspersky Anti-Virus
ods	Sous-système d'analyse à la demande
oas	Sous-système de protection en temps réel des fichiers
qb	Sous-système de la quarantaine et du dossier de sauvegarde
scandll	Module auxiliaire de l'analyse Anti-Virus
core	Sous-système de la fonction antivirus de base
avscan	Sous-système de traitement antivirus
avserv	Sous-système d'administration du moteur antivirus
prague	Sous-système de fonction de base
scsrv	Sous-système de gestion des requêtes émanant de l'intercepteur de scripts
script	Intercepteur de scripts
updater	Sous-système de mise à jour des bases et des modules d'application

B.1.10. Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus

Paramètre	Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus (**Créer des fichiers de vidage sur incident**)
Description	Le paramètre **Création de fichiers de vidage des processus de Kaspersky Anti-Virus** appartient au groupe de paramètres **Interaction avec l'utilisateur**. Si un problème survient durant l'utilisation de Kaspersky Anti-Virus (par exemple, Kaspersky Anti-Virus s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez activer la création de fichiers de vidage de mémoire des processus de Kaspersky Anti-Virus et envoyer ces fichiers au service d'assistance technique de Kaspersky Lab pour analyse. Pour obtenir de plus amples informations sur la manière de contacter le service d'assistance technique, consultez consultez le point 1.2.3 à la page 24.

Valeurs et certaines recommandations quant à leur utilisation	Les fichiers de vidages sont créés / ne sont pas créés.
	Pour activer la création de fichiers de vidage, indiquez le dossier où ces fichiers seront enregistrés.
	Remarque
	Si vous saisissez un chemin d'accès à un répertoire inexistant, les fichiers de vidage ne seront pas créés.
	Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via une console Kaspersky Anti-Virus dans MMC installée sur un autre ordinateur, vous devrez indiquer les paramètres des fichiers de vidage dans la clé de registre suivante puis fermer et ouvrir à nouveau la console de Kaspersky Anti-Virus dans MMC afin d'activer le vidage du processus de la console de Kaspersky Anti-Virus dans MMC.
	• Si une version 32 bits de Microsoft Windows est installée sur le serveur protégé :
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp`

	• Si une version 64 bits de Microsoft Windows est installée sur le serveur protégé :
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\Enable=0x00000000`
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\Folder=C:\Temp`
	`0x00000000` : active la création de fichiers de vidage du processus de la console de Kaspersky Anti-Virus dans MMC ;
	`0x00000001`: désactive la création de fichiers de vidage du processus de la console de Kaspersky Anti-Virus dans MMC ;
	`Folder=C:\Temp` : répertoire dans lequel le fichier de vidage du processus de la console de Kaspersky Anti-Virus dans MMC sera enregistré après un arrêt sur incident.

Valeur par défaut	Les fichiers de vidage ne sont pas créés.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 3.2, page 46 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.2, p. 303.

B.2. Paramètres de planification des tâches

Vous pouvez configurer les paramètres de planification des tâches suivants.

- La fréquence (cf. point B.2.1, p. 392) ;
- La date d'entrée en vigueur de la planification et l'heure d'exécution de la tâche (cf. point B.2.2, p. 393) ;
- La date de la fin de validité de la planification (cf. point B.2.3, p. 394) ;
- La durée maximale de l'exécution d'une tâche (cf. point B.2.4, p. 395) ;
- L'intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue (cf. point B.2.5, p. 395) ;
- Le lancement des tâches non exécutées (cf. point B.2.6, p. 396) ;

- La répartition des lancements dans l'intervalle, min. (cf. point B.2.7, p. 397).

B.2.1. Fréquence

Paramètre	Fréquence d'exécution
Description	Ce paramètre est obligatoire. La tâche peut être exécutée selon une fréquence que vous définirez en heures, en jours ou en semaines, les jours indiqués de la semaine, après le lancement de Kaspersky Anti-Virus, la mise à jour des bases ou la récupération des mises à jour par le serveur d'administration.
Valeurs et certaines recommandations quant à leur utilisation	Les valeurs possibles sont : • **Chaque heure**. La tâche sera exécutée selon la fréquence horaire que vous avez définie. • **Chaque jour**. La tâche sera exécutée selon la fréquence journalière que vous avez définie. • **Chaque semaine**. La tâche sera exécutée selon la fréquence hebdomadaire que vous avez définie. • **Au lancement de l'application**. La tâche sera lancée chaque fois que Kaspersky Anti-Virus sera ouvert. • **À la mise à jour de la base antivirus** (cette option ne s'applique pas aux tâches de mise à jour). La tâche sera exécutée après chaque mise à jour des bases de Kaspersky Anti-Virus. • **Après réception des mises à jour par le serveur d'administration** (s'applique uniquement aux tâches **mise à jour des bases de l'application**, **Mise à jour des modules de l'application** et **Copie des mises à jour**, s'affiche uniquement dans la console d'administration Kaspersky Administration Kit, ne s'affiche pas dans la console de Kaspersky Anti-Virus dans MMC). La tâche sera lancée chaque fois que le serveur d'administration reçoit la mise à jour des bases.
Valeur par défaut	Dans les tâches prédéfinies locales, les valeurs par défaut du paramètre **Fréquence** sont les suivantes : • Protection en temps réel des fichiers : Au lancement de l'application ; • Analyse des scripts : au lancement de l'application ; • Analyse au démarrage du système : au lancement de l'appli-

	cation ; • Analyse de l'intégrité de l'application : au lancement de l'application ; • Analyse complète de l'ordinateur : chaque semaine (le vendredi à 20 h00) ; • Analyse des objets en quarantaine : à la mise à jour de la base antivirus ; • Mise à jour des bases de l'application **:** toutes les heures ; • Mise à jour des modules de l'application : chaque semaine (le vendredi à 16h00) ; • Copie des mises à jour : planification désactivée ; • Remise des bases de l'application à l'état antérieur : la planification n'est pas prévue ; Dans les tâches d'analyse à la demande recréées par les utilisateurs, la planification est désactivée.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.2. Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche

Paramètre	Date d'entrée en vigueur de la planification et heure de la première exécution de la tâche
Description	Les paramètres suivants sont obligatoires. • **Date d'entrée en vigueur de la planification (A partir du)**. A partir de la date que vous aurez saisie, Kaspersky Anti-Virus exécutera la tâche selon la fréquence définie. • **A partir du** (appliquée si la valeur du paramètre **Fréquence** est **Chaque heure**). Kaspersky Anti-Virus exécutera la tâche

	pour la première fois à l'heure indiquée. • **Démarrer à** (appliquée si la valeur du paramètre **Fréquence** est **Chaque heure** ou **Chaque semaine**). Kaspersky Anti-Virus lancera la tâche à l'heure indiquée selon la fréquence définie par le paramètre **Fréquence**.
Valeurs possibles	Indiquez la date et l'heure
Valeur par défaut	Dans les tâches d'analyse à la demande recréées par les utilisateurs, ces paramètres sont désactivés. Dans les tâches prédéfinies locales, les valeurs par défaut de ces paramètres sont les suivantes : • Analyse complète de l'ordinateur : tous les vendredi à 20h00 selon la configuration de l'heure sur le serveur protégé ; • Mise à jour des bases de l'application toutes les trois heures. Ces paramètres sont désactivés par défaut dans la planification des autres tâches prédéfinies.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.3. Date de la fin de validité de la planification

Paramètre	Date de la fin de validité de la planification (**Date finale de planification**)
Description	La planification ne sera plus en vigueur à partir de la date que vous aurez saisie : la tâche programmée ne sera pas exécutée. Ce paramètre ne s'applique pas si la valeur du paramètre **Fréquence** est **Au lancement de l'application** ou **À la mise à jour de la base antivirus**.
Valeurs possibles	Saisissez la date ou sélectionnez-la dans la boîte de dialogue **Calendrier**

Valeur par défaut	Non définie

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.4. Durée maximale de l'exécution d'une tâche

Paramètre	Durée maximale de l'exécution d'une tâche
Description	Si l'exécution de la tâche dépasse le nombre d'heures et de minutes que vous avez défini, elle sera interrompue par Kaspersky Anti-Virus. Une tâche interrompue de cette manière ne sera pas considérée comme une tâche non-exécutée. Ce paramètre vous permet d'instaurer une heure d'arrêt automatique des tâches de la protection en temps réel. Ce paramètre ne concerne pas les tâches de mise à jour.
Valeurs possibles	Définissez le nombre d'heures et de minutes
Valeur par défaut	Désactivé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.5. Intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue

Paramètre	L'intervalle de temps au cours d'une journée pendant lequel la tâche sera suspendue (**Pause à partir de... jusqu'à**)
Description	Le cas échéant, vous pouvez suspendre une tâche pendant un intervalle donné au cours d'une journée, par exemple suspendre l'analyse à la demande lorsque la charge du serveur à ce moment est élevée et que vous ne souhaitez pas contribuer à l'augmentation de la charge en exécutant cette tâche. Ce paramètre ne concerne pas les tâches de mise à jour. Si en plus de ce paramètre vous activez le paramètre **Durée maximale de l'exécution d'une tâche**, n'oubliez pas que l'intervalle de suspension de la tâche indiqué entre dans la durée maximale d'exécution de la tâche.
Valeurs possibles	Définissez les intervalles de temps au cours de la journée
Valeur par défaut	Non défini

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.6. Lancement des tâches non exécutées

Paramètre	Lancement des tâches non exécutées
Description	Vous pouvez activer le lancement des tâches non exécutées. Si Kaspersky Anti-Virus ne peut lancer la tâche à l'heure indiquée (par exemple, l'ordinateur est éteint), Kaspersky Anti-Virus consi-

	dère cette tâche comme *non exécutée* et l'exécute automatiquement dès qu'il sera à nouveau lancé. Ce paramètre ne s'applique pas si la valeur du paramètre **Fréquence** est **Au lancement de l'application** ou **À la mise à jour de la base antivirus**.
Valeurs possibles	Activé/désactivé
Valeur par défaut	Désactivé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.2.7. Répartition des lancements dans l'intervalle, min

Paramètre	Répartition des lancements dans l'intervalle, min
Description	Si vous définissez ce paramètre, alors la tâche sera exécutée de manière aléatoire dans l'intervalle compris entre l'heure de lancement prévue et l'heure de lancement prévue plus la valeur de ce paramètre. Vous pouvez utiliser ce paramètre si, par exemple, vous utilisez un ordinateur intermédiaire pour la diffusion des mises à jour vers de nombreux serveurs et ce, afin de réduire la charge de l'ordinateur intermédiaire et le trafic de réseau. Ce paramètre n'est pas appliqué si vous avez choisi le type d'exécution Au lancement de l'application, Après la mise à jour des bases ou Après la récupération des mises à jour par le serveur d'administration.
Valeurs possibles	Saisissez le nombre de minutes

Valeur par défaut	Non défini

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 5.7.1 à la page 60 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.3. Paramètres de protection dans la tâche *Protection en temps réel des fichiers* et dans les tâches d'analyse à la demande

Les paramètres de sécurité suivants concernent la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande :

- Mode de protection des objets (uniquement dans la tâche **Protection en temps réel des fichiers**) (cf. point B.3.1 à la page 399) ;
- Les objets à analyser (cf. point B.3.2, p. 400) ;
- L'analyse uniquement des objets neufs ou modifiés (cf. point B.3.3, p. 402) ;
- L'analyse des objets composés (cf. point B.3.4, p. 402) ;
- Les actions à exécuter sur les objets infectés (cf. point B.3.5, p. 404) ;
- Les actions à exécuter sur les objets suspects (cf. point B.3.6, p. 406) ;
- Les actions à exécuter sur les objets en fonction du type de menace (cf. point B.3.7, p. 408) ;
- L'exclusion des objets (cf. point B.3.8, p. 410) ;
- L'exclusion des menaces (cf. point B.3.9, p. 411) ;
- La durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413) ;

- La taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413) ;
- L'application de la technologie iChecker (cf. point B.3.12, p. 414) ;
- L'application de la technologie iSwift (cf. point B.3.13, p. 415).

B.3.1. Mode de protection

Le paramètre de sécurité **Mode de protection** concerne uniquement la tâche **Protection en temps réel des fichiers**.

Paramètre	Mode de protection
Description	Ce paramètre concerne uniquement la tâche **Protection en temps réel des fichiers**. Il définit le type d'accès aux objets qui entraînera une analyse de Kaspersky Anti-Virus. Le paramètre **Mode de protection** possède une valeur unique pour toutes les couvertures d'analyse reprises dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les nœuds particuliers.
Valeurs et certaines recommandations quant à leur utilisation	Sélectionnez un des modes de protection en fonction de vos exigences de sécurité pour le système, des types de formats de fichiers enregistrés sur le serveur et du type d'informations qu'ils renferment : • **Mode intelligent**. Kaspersky Anti-Virus analyse l'objet à l'ouverture et le vérifie à nouveau après l'enregistrement, si l'objet a été modifié. Si le processus pendant son exécution contacte plusieurs fois l'objet et le modifie, Kaspersky Anti-Virus le vérifiera à nouveau uniquement après la dernière sauvegarde par ce processus. • **À l'accès et en cas de modification**. Kaspersky Anti-Virus analyse l'objet à l'ouverture et le vérifie à nouveau à la fermeture s'il a été modifié. • **À l'accès**. Kaspersky Anti-Virus analyse l'objet à l'ouverture aussi bien en écriture qu'en exécution ou en modification. • **À l'exécution**. Kaspersky Anti-Virus analyse l'objet uniquement en cas d'ouverture pour exécution. Par défaut, les objets sont analysés en mode de protection **A l'accès et à la modification**.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 6.2.3 à la page 90 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.3.2. Objets à analyser

Le paramètre de sécurité **Objets analysés** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Objets à analyser
Description	Ce paramètre définit si tous les objets de la couverture de protection seront analysés ou uniquement les objets d'un format ou dotés d'une extension défini. Les experts de Kaspersky Lab composent des listes des formats et des extensions qui peuvent contenir des objets susceptibles d'être infectés. Ces listes sont reprises dans les bases de Kaspersky Anti-Virus. Quand elles sont actualisées chez Kaspersky Lab, vous les recevez en même temps que la mise à jour des bases. Grâce au paramètre **Objets à analyser**, vous pouvez composer votre propre liste des extensions.
Valeurs et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Analyser tous les objets**. Kaspersky Anti-Virus analyse tous les objets, quel que soit leur format ou leur extension ; • **Objets analysés en fonction du format**. Avant d'analyser l'objet, Kaspersky Anti-Virus définit son format. Si le format figure dans la liste des formats des objets pouvant être infectés, l'objet sera analysé par Kaspersky Anti-Virus. Si le format ne figure pas dans cette liste (par exemple, un fichier txt ne peut être infecté), alors Kaspersky Anti-Virus ne l'analyse pas ; • **Objets analysés en fonction d'une liste d'extensions**. Kaspersky Anti-Virus analyse uniquement les objets dont l'extension figure dans la liste des extensions d'objets pouvant être infectés. Si l'extension de l'objet ne figure pas dans cette liste, Kaspersky Anti-Virus l'ignorera. Si vous sélectionnez la valeur **Objets en fonction de la liste définie des extensions**, la vitesse d'analyse sera plus rapide que si vous choisissez la valeur **Objets en fonction du for-**

	mat. Toutefois, le risque d'infection sera supérieur car l'extension d'un objet ne correspond pas toujours à son format. Par exemple, un fichier portant l'extension .txt n'est pas nécessairement un fichier au format texte. Il peut s'agir d'un fichier exécutable contenant une menace. Mais Kaspersky Anti-Virus n'analysera pas l'objet car l'extension .txt ne figure pas dans la liste des extensions des objets pouvant être infectés. • **Objets analysés en fonction de masques d'extensions**. Kaspersky Anti-Virus analyse les objets dont les extensions figurent dans la liste indiquée (par défaut, cette liste est vide). Vous pouvez ajouter des extensions ou des masques d'extension à la liste ainsi que supprimer des extensions ou des masques existants. Les masques d'extension acceptent les caractères suivants : * et ?. Vous pouvez ajouter toutes les extensions de la liste des extensions livrée avec Kaspersky Anti-Virus. Pour ce faire, cliquez sur le bouton **Valeur par défaut** dans la boîte de dialogue de modification de la liste. **Analyser les secteurs d'amorçage et la partition MBR.** Ce paramètre intervient si la couverture d'analyse contient les couvertures prédéfinies **Disques durs** et **Disques amovibles**, la couverture prédéfinie **Poste de travail** ou des disques créés dynamiquement. Ce paramètre n'intervient pas si la couverture d'analyse contient uniquement **Mémoire système**, **Objets exécutés au démarrage du système**, **Dossiers partagés** ou si la couverture d'analyse contient des fichiers ou des dossiers distincts. **Analyser les flux NTFS alternatifs**. Kaspersky Anti-Virus analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 6.2.3 à la page 90 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.3 à la page 345.

B.3.3. Analyse uniquement des objets neufs et modifiés

Le paramètre de protection **Analyse uniquement des objets neufs et modifiés** est appliqué dans la tâche **Protection en temps réel des fichiers** et dans les tâches d'analyse à la demande.

Paramètre	**Analyse uniquement des objets neufs et modifiés**
Description	Quand l'analyse uniquement des objets neufs et modifiés est activée, Kaspersky Anti-Virus analyse tous les objetsde la couverture d'analyse désignée sauf ceux qu'il a analysé une fois, qui n'étaient pas infectés et qui n'ont pas changé depuis cette analyse.
Valeurs et certaines recommandations quant à leur utilisation	**Activer** / **Désactiver**

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.4. Traiter les objets composés

Le paramètre de sécurité **Traiter les objets composés** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Traiter les objets composés
Description	L'analyse des objets composés dure un certain temps. Par défaut, Kaspersky Anti-Virus analyse uniquement les objets composés les plus souvent infectés ou qui représentent le plus grand danger pour le serveur en cas d'infection. Les objets composés des autres types ne sont pas analysés. Ce paramètre vous permet, conformément à vos exigences de

	sécurité, de sélectionner les types d'objets composés qui seront analysés par Kaspersky Anti-virus.
Valeurs et certaines recommandations quant à leur utilisation	Choisissez une ou plusieurs des valeurs suivantes : • **Archives**. Kaspersky Anti-Virus analyse les archives traditionnelles. N'oubliez pas que Kaspersky Anti-Virus découvre les menaces dans les archives de la majorité des types mais il peut réparer uniquement les archives ZIP, ARJ, RAR et CAB ; • **Archives SFX**. Kaspersky Anti-Virus analyse le module de décompactage des archives SFX (auto-extractibles) ; • **Bases de données de messagerie**. Kaspersky Anti-Virus analyse les fichiers des bases de données de messagerie de Microsoft Office Outlook et Microsoft Outlook Express ; • **Objets compactés**. Kaspersky Anti-Virus analyse les fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack. Les objets composés de ce type contiennent plus souvent que d'autres des menaces ; • **Message de texte plat**. Kaspersky Anti-Virus analyse les messages de texte plat, par exemple les messages de Microsoft Office Outlook ou Microsoft Outlook Express ; • **Objets OLE intégrés**. Kaspersky Anti-Virus analyse les objets intégrés dans les documents Microsoft Office. Les documents Microsoft Office contiennent souvent des objets exécutables qui peuvent renfermer des menaces. Si pour la zone de sécurité sélectionnée, le paramètre **Analyse uniquement des objets neufs et modifiés** est désactivée, alors vous pouvez activer ou désactiver l'analyse uniquement des objets neufs et modifiés pour chaque type d'objet composé séparément. Quand l'analyse uniquement des objets neufs et modifiés est activée, Kaspersky Anti-Virus analyse tous les objetsde la couverture d'analyse désignée sauf ceux qu'il a analysé une fois, qui n'étaient pas infectés et qui n'ont pas changé depuis cette analyse.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.5. Actions à exécuter sur les objets infectés

Le paramètre de sécurité **Action à exécuter sur les objets** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

B.3.5.1. Dans la tâche *Protection en temps réel des fichiers*

Paramètre	Actions à exécuter sur les objets infectés
Description	Lorsque Kaspersky Anti-Virus identifie un objet comme étant infecté, il bloque l'accès à ce dernier pour l'application qui le sollicitait et exécute l'action que vous avez définie. Avant de modifier l'objet (ou de le réparer ou de le supprimer), Kaspersky Anti-Virus place une copie de l'objet en sauvegarde, le dossier spécial prévu pour la conservation des objets sous forme cryptées. Pour obtenir de plus amples informations sur la sauvegarde, consultez le Chapitre 12 à la page 190. Kaspersky Anti-Virus ne tentera pas de réparer ou de supprimer un objet s'il ne parvient pas d'abord à placer sa copie en sauvegarde. L'objet n'est pas modifié. Vous pouvez voir la raison pour laquelle l'objet n'a pas été modifié dans le rapport détaillé sur l'exécution de la tâche.
Valeurs de paramètres et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Interdire l'accès + réparer**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il laisse l'objet inchangé (l'application qui avait sollicité le fichier ne peut y accéder) ; • **Interdire l'accès + réparer, supprimer si la réparation est impossible**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il le supprime ; • **Interdire l'accès + supprimer**. Kaspersky Anti-Virus supprime l'objet infecté ; • **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute automatiquement les actions sur l'objet en fonction des données sur le danger que représentent les menaces identifiées et des possibilités de réparation ; par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie

	car ils ne s'intègrent pas à d'autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés ; • **Interdire l'accès**. L'objet n'est pas modifié. Kaspersky Anti-Virus ne tente pas de réparer ou de supprimer l'objet et se contente d'en interdire l'accès.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 6.2.2.2 à la page 82 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.5.2. Dans les tâches d'analyse à la demande

Paramètre	Actions à exécuter sur les objets infectés
Description	Quand Kaspersky Anti-Virus identifie un objet infecté, il exécute l'action que vous avez définie. Avant de modifier l'objet (ou de le réparer ou de le supprimer), Kaspersky Anti-Virus place une copie de l'objet en sauvegarde, le dossier spécial prévu pour la conservation des objets sous forme cryptées. Pour obtenir de plus amples informations sur la sauvegarde, consultez le Chapitre 12 à la page 190. Kaspersky Anti-Virus ne tentera pas de réparer ou de supprimer un objet s'il ne parvient pas d'abord à placer sa copie en sauvegarde. L'objet n'est pas modifié. Vous pouvez voir la raison pour laquelle l'objet n'a pas été modifié dans le rapport détaillé sur l'exécution de la tâche.
Valeurs de paramètres et certaines recommandations quant à leur utilisation	Choisissez une des valeurs suivantes : • **Réparer**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, l'objet n'est pas modifié ; • **Réparer, supprimer si la réparation est impossible**. Kaspersky Anti-Virus tente de réparer l'objet et si la réparation est impossible, il le supprime ; • **Supprimer**. Kaspersky Anti-Virus supprime directement l'objet sans tenter de le réparer ; • **Exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute automatiquement les actions sur

	l'objet en fonction des données sur le danger que représentent les menaces identifiées et des possibilités de réparation ; par exemple, Kaspersky Anti-Virus supprime directement les chevaux de Troie car ils ne s'intègrent pas à d'autres fichiers et ne les infectent pas et par conséquent, ils ne peuvent être réparés ; • **Ignorer**. L'objet n'est pas modifié. Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Les informations relatives à la découverte de l'objet infecté sont consignées dans le rapport détaillé sur l'exécution de la tâche.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.6. Actions à exécuter sur les objets suspects

Le paramètre de sécurité **Actions à exécuter sur les objets suspects** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

B.3.6.1. Dans la tâche *Protection en temps réel des fichiers*

Paramètre	Actions à exécuter sur les objets suspects
Description	Quand Kaspersky Anti-Virus identifie un objet suspect, il empêche l'application d'accéder à l'objet et exécute sur celui-ci l'action que vous aurez définie. Avant de supprimer l'objet, Kaspersky Anti-Virus place une copie de l'objet en sauvegarde, le dossier spécial prévu pour la conservation des objets sous forme cryptée. Pour obtenir de plus amples informations sur la sauvegarde, consultez le Chapitre 12 à la page 190.
Valeurs et	Choisissez une des valeurs suivantes :

certaines recommandations quant à leur utilisation	• **Interdire l'accès + quarantaine**. L'objet est placé dans un dossier spécial (la quarantaine) où il est crypté. Pour obtenir de plus amples informations sur la quarantaine, consultez le Chapitre 11 à la page 171 ; • **Interdire l'accès + supprimer**. Kaspersky Anti-Virus supprime l'objet suspect du disque ; Kaspersky Anti-Virus ne supprime pas objet s'il ne parvient pas d'abord à placer sa copie en quarantaine. L'objet n'est pas modifié. Vous pouvez voir la raison pour laquelle l'objet n'a pas été modifié dans le rapport détaillé sur l'exécution de la tâche. • **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute les actions sur l'objet en fonction des données sur le danger que représente la menace identifiée dans l'objet ; • **Interdire l'accès**. L'objet n'est pas modifié : Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Il se contente d'en interdire l'accès.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 6.2.2.2 à la page 82 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.6.2. Dans les tâches d'analyse à la demande

Paramètre	Actions à exécuter sur les objets suspects
Description	Quand Kaspersky Anti-Virus identifie un objet suspect, il exécute l'action que vous avez définie. Avant de supprimer l'objet, Kaspersky Anti-Virus place une copie de l'objet en sauvegarde, le dossier spécial prévu pour la conservation des objets sous forme cryptée. Pour obtenir de plus amples informations sur la sauvegarde, consultez le Chapitre 12 à la page 190.
Valeurs et certaines recommandations quant à leur	Choisissez une des valeurs suivantes : • **Quarantaine**. L'objet est placé dans un dossier spécial (la quarantaine) où il est crypté. Pour obtenir de plus amples informations sur la quarantaine, consultez le Chapitre 11 à la page 171 ;

utilisation	• **Supprimer**. Kaspersky Anti-Virus supprime l'objet suspect du disque. Kaspersky Anti-Virus ne supprime pas objet s'il ne parvient pas d'abord à placer sa copie en quarantaine. L'objet n'est pas modifié. Vous pouvez voir la raison pour laquelle l'objet n'a pas été modifié dans le rapport détaillé sur l'exécution de la tâche. • **Interdire l'accès + exécuter l'action recommandée**. Kaspersky Anti-Virus sélectionne et exécute les actions sur l'objet en fonction des données sur le danger que représente la menace identifiée dans l'objet ; • **Interdire l'accès**. L'objet n'est pas modifié : Kaspersky Anti-Virus ne tente pas de le réparer ou de le supprimer. Les informations relatives à l'objet suspect identifié sont consignées dans le rapport détaillé sur l'exécution de la tâche.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.7. Actions en fonction du type de menace

Le paramètre de sécurité **Actions en fonction du type de menace** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Actions en fonction du type de menace (**Agir en fonction du type de menace**)
Description	Les menaces de certains types représentent un plus grand danger pour le serveur que d'autres. Par exemple, un cheval de Troie peut causer bien plus de dégâts qu'un logiciel publicitaire. A l'aide des paramètres de ce groupe, vous pouvez configurer diverses actions de Kaspersky Anti-Virus pour les objets qui contiennent les menaces de différents types. Quand vous définissez les valeurs de ce paramètres, Kaspersky Anti-Virus les appliquera en même temps que les paramètres **Actions à exécuter sur les objets infectés** et **Actions à exécuter sur les objets suspects**.

Valeurs et certaines recommandations quant à leur utilisation	Pour chaque type de menaces, sélectionnez dans la liste des actions qui pourront être exécutées sur les objets infectés et suspects deux actions que Kaspersky Anti-Virus tentera d'exécuter s'il découvre une menace du type précisé dans l'objet. Kaspersky Anti-Virus exécutera la deuxième action sur l'objet s'il ne parvient pas à exécuter la première. Kaspersky Anti-Virus appliquera les actions définies aussi bien aux objets suspects qu'aux objets infectés si cela est possible. Ainsi, si vous sélectionnez **Réparer** en guise de première action et **Quarantaine** en guise de deuxième, Kaspersky Anti-Virus mettra l'objet infecté en quarantaine s'il ne parvient pas à le réparer et il placera l'objet suspect directement en quarantaine en ignorant l'action **Réparer** car les objets suspects ne sont pas soumis à la réparation. Si vous sélectionnez **Ignorer** en guise de première action, alors la deuxième action ne pourra être appliquée. Pour les autres valeurs, il est conseillé de définir deux actions. N'oubliez que les menaces du type *Vers de réseau* et *Vers classiques* sont regroupés, dans la liste des catégories de menaces, sous la même appellation *Virus*. Si Kaspersky Anti-Virus ne parvient pas à placer l'objet en sauvegarde ou en quarantaine, alors il ne réalisera pas l'action sur l'objet (par exemple, la réparation ou la suppression). L'objet est considéré comme ignoré. Vous pouvez voir la raison pour laquelle l'objet a été ignoré dans le rapport détaillé sur l'exécution de la tâche. Dans la liste des types de menace, la valeur **Non défini** inclut les nouveaux virus qui ne figurent actuellement dans aucun des types connus. Les types de menaces sont décrits au point 1.1.2 à la page 16.
Valeur par défaut	Désactivé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.8. Exclusion des objets

Le paramètre de sécurité **Exclusion des objets** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Exclusion des objets (**Exclure des objets**)
Description	Ce paramètre vous permet d'exclure de l'analyse des fichiers distincts ou plusieurs fichiers à l'aide d'un masque de nom de fichier. En excluant les fichiers de grande taille de l'analyse, vous pouvez augmenter le volume de fichiers et réduire la durée d'exécution de l'analyse à la demande. Les informations relatives à l'exclusion d'un objet de l'analyse sont reprises dans le rapport détaillé sur l'exécution de la tâche (conformément aux paramètres par défaut des rapports). Pour obtenir de plus amples informations sur les rapports, consultez le point 13.2 à la page 205. Dans les tâches d'analyse à la demande, quand Kaspersky Anti-Virus analyse un processus dans la mémoire, il analyse également le fichier de lancement du processus même si ce fichier figure dans la liste des exclusions.
Valeurs et certaines recommandations quant à leur utilisation	Composez la liste des fichiers. Vous pouvez saisir le nom du fichier en entier ou à l'aide d'un masque. Pour définir les masques, utilisez les caractères * et ?.
Valeur par défaut	La liste est vide

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.9. Exclusion des menaces

Le paramètre de sécurité **Exclusion des menaces** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Exclusion des menaces
Description	Si Kaspersky Anti-Virus détermine qu'un objet analysé est infecté ou suspect et qu'il exécute des actions sur celui-ci alors que vous estimez que cet objet ne présente aucun danger pour le serveur, vous pouvez exclure la menace découverte dans l'objet de la liste des menaces que Kaspersky Anti-Virus peut traiter. Vous pouvez exclure une menace selon son nom dans un objet particulier ou toute une catégorie de menaces. Si vous excluez une menace, Kaspersky Anti-Virus considère que l'objet qui contient cette menace est sain.

Valeurs et certaines recommandations quant à leur utilisation	Composez la liste des menaces à exclure (la liste est vide par défaut). Séparez les valeurs dans la liste par un point virgule (;). Pour exclure un objet de l'analyse, indiquez le nom complet de la menace découverte dans cet objet; – de Kaspersky Anti-Virus indique que l'objet est infecté ou suspect. Le nom complet de la menace est défini dans les résultats de l'analyse de l'objet. Il peut contenir les informations suivantes : **<classe de menace>:<type de menace>.<abréviation de la plateforme>.<nom de la menace>.<code de modification de la menace>**. Admettons que vous utilisez l'utilitaire Remote Administrator en guise d'outil d'administration à distance. La majorité des logiciels antivirus classe le code de cet utilitaire dans les menaces du type *Riskware*. Afin que Kaspersky Anti-Virus ne le bloque pas, ajoutez le nom complet de la menace dans la liste des menaces exclues du noeud de l'arborescence des ressources fichiers du serveur où se trouvent les fichiers de l'utilitaire. Vous pouvez attribuer les valeurs suivantes au paramètre : • Nom complet de la menace : **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus n'exécutera pas les actions uniquement sur les modules dans lesquels il trouve la menace baptisée Win32.RAdmin.20. • Masque du nom complet de la menace : **not-virus:RemoteAdmin.*** Kaspersky Anti-Virus n'exécutera pas les actions sur les programmes Remote Administrator de n'importe quelle version. • Masque du nom complet de la menace, avec uniquement le type de menace : **not-a-virus:*** Kaspersky Anti-Virus n'exécutera aucune action sur tous les objets contenant des menaces de ce type. Vous pouvez obtenir le nom complet de la menace découverte dans le logiciel dans le rapport détaillé de l'exécution de la tâche. Pour obtenir de plus amples informations sur les rapports, consultez le point 13.2 à la page 205. Vous pouvez également trouver le nom complet de la menace découverte dans l'objet sur le site de l'Encyclopédie des virus Viruslist.com Pour trouver le nom de la menace, saisissez le nom du logiciel dans le champ **Rechercher**.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.10. Durée maximale de l'analyse d'un objet

Le paramètre de sécurité **Durée maximale de l'analyse d'un objet** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Durée maximale de l'analyse d'un objet, s. (**Arrêter si l'analyse dure plus de... sec**)
Description	Kaspersky Anti-Virus arrête l'analyse si celle-ci dure plus longtemps que la valeur définie (en secondes) pour le paramètre. Les informations relatives à l'exclusion d'un objet de l'analyse sont reprises dans le rapport détaillé sur l'exécution de la tâche (conformément aux paramètres par défaut des rapports).
Valeurs	Saisissez la durée maximale, en secondes, de l'analyse d'un objet.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.11. Taille maximale de l'objet composé à analyser

Le paramètre de sécurité **Taille maximale de l'objet composé à analyser** concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Taille maximale de l'objet composé à analyser, Mo (**Ne pas analyser les objets composés de plus de...Mo**)
Description	Si la taille de l'objet composé à analyser dépasse la valeur définie, Kaspersky Anti-Virus l'ignorera. Les informations relatives au fait qu'un objet a été ignoré sont reprises dans le rapport détaillé sur l'exécution de la tâche (conformément aux paramètres par défaut des rapports)
Valeurs	Définissez la taille maximale de l'objet composé en mégaoctets

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.12. Application de la technologie iChecker

Le paramètre de sécurité Activer iChecker concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Application de la technologie iChecker (**Utiliser la technologie iChecker**)
Description	Ce paramètre active ou désactive l'application de la technologie iChecker développée par Kaspersky Lab. La technologie iChecker s'applique uniquement aux objets de type et de format pouvant être infectés. La technologie iChecker permet de ne pas analyser une nouvelle fois les objets du serveur considérés comme non infectés par Kaspersky Anti-Virus à l'issue des analyses antérieures. Le recours à la technologie iChecker diminue la charge du processeur et des systèmes du disque et accélère la vitesse de l'analyse ainsi que l'échange de données. N'oubliez pas que Kaspersky Anti-Virus analyse à nouveau un objet si ce dernier a été modifié depuis la dernière analyse, si le niveau de protection a été augmenté. Kaspersky Anti-Virus consignera dans le rapport que l'objet n'a

	pas été analysé suite à l'application de la technologie iChecker (conformément aux paramètres par défaut des rapports).
Valeurs	Activée / désactivée

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.3.13. Application de la technologie iSwift

Le paramètre de sécurité Application de la technologie iSwift concerne la tâche **Protection en temps réel des fichiers** et les tâches d'analyse à la demande.

Paramètre	Application de la technologie iSwift (**Utiliser la technologie iSwift**)
Description	Ce paramètre active ou désactive l'application de la technologie iSwift développée par Kaspersky Lab. La technologie iSwift concerne tous les objets du système de fichiers NTFS. La technologie iSwift permet de ne pas analyser à nouveau les objets qui à l'issue des analyses précédentes ont été reconnus comme sains par Kaspersky Anti-Virus ainsi que les objets analysés par d'autres applications antivirus de Kaspersky Lab de la version 6.0. Le recours à la technologie iSwift diminue la charge du processeur et des systèmes du disque et accélère la vitesse de l'analyse ainsi que l'échange de données. N'oubliez pas que Kaspersky Anti-Virus analyse à nouveau un objet si ce dernier a été modifié depuis la dernière analyse, si le niveau de protection a été augmenté. Kaspersky Anti-Virus consignera dans le rapport que l'objet n'a pas été analysé suite à l'application de la technologie iSwift (conformément aux paramètres par défaut des rapports). Kaspersky Anti-Virus exploite iNetSwift, une version de réseau de la technologie iSwift. Elle fonctionne comme la technologie normale et permet de ne pas devoir traiter les fichiers en prove-

	nance d'autres ordinateurs sur lesquels est installé une des applications suivantes et où fonctionne iSwift. • Kaspersky Anti-Virus 6.0 for Windows Workstations ; • Kaspersky Anti-Virus 6.0 for Windows Servers ; • Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition ; • Kaspersky Anti-Virus 6.0 / 7.0 ; • Kaspersky Internet Security 6.0 / 7.0. L'application de iNetSwift empêche le nouveau traitement des objets dans le cadre du réseau et réduit au minimum l'impact de Kaspersky Anti-Virus sur la vitesse d'échange des fichiers. Si le serveur protégé est doté de Novell Client For Windows XP/2003 version 4.71 ou suivante, la technologie iSwift fonctionne uniquement dans le cadre d'un ordinateur sans utiliser la version de réseau.
Valeurs	Activée / désactivée

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus, dans la tâche **Protection en temps réel des fichiers** – cf. point 6.2.2.2, p. 82 ; dans la tâche d'analyse à la demande – cf. point 9.2.2.2 à la page 136 ;
- Dans l'application Kaspersky Administration Kit, cf. point 19.3 à la page 294.

B.4. Paramètres d'interdiction automatique de l'accès des ordinateurs au serveur

Cette annexe décrit les paramètres suivants de blocage automatique de l'accès des ordinateurs au serveur :

- L'activation/la désactivation du blocage automatique l'accès depuis les ordinateurs (cf. point B.4.1, p. 417) ;
- Les actions à exécuter sur les ordinateurs infectés (cf. point B.4.2, page 417) ;
- La liste des ordinateurs exclus du blocage (cf. point B.4.3, p. 419) ;

- Prévention des épidémies virales (cf. point B.4.4, p. 419).

B.4.1. Activation / désactivation de l'interdiction de l'accès des ordinateurs au serveur

Paramètre	Activation / désactivation de l'interdiction de l'accès des ordinateurs au serveur
Description	Ce paramètre active ou désactive le blocage automatique de l'accès depuis les ordinateurs en cas de tentative d'écriture d'un fichier infecté ou suspect sur le serveur. Kaspersky Anti-Virus ne bloque pas automatiquement l'accès des ordinateurs, même si la tâche **Protection en temps réel des fichiers** possède le paramètre **Mode de protection** dont la valeur est **À l'accès** ou **À l'exécution**. Dans ce cas, vous pouvez interdire l'accès de l'ordinateur manuellement. Si vous activez la fonction d'interdiction automatique de l'accès des ordinateurs, elle sera effective uniquement lors de l'exécution de la tâche **Protection en temps réel des fichiers**.
Valeurs possibles	Activer/désactiver
Valeur par défaut	Désactivé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 7.2 à la page 98 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.3.1 à la page 308.

B.4.2. Actions à exécuter sur les ordinateurs infectés

Paramètre	Actions à exécuter sur les ordinateurs infectés

Description	Si la fonction d'interdiction automatique est activée, alors dès qu'un ordinateur quelconque du réseau local tente d'écrire un fichier suspect ou infecté sur le serveur protégé, Kaspersky Anti-Virus exécutera les actions que vous aurez définies. Vous avez le choix entre deux actions : • **Interdire l'accès des ordinateurs au serveur**. Kaspersky Anti-Virus interdit l'accès de l'ordinateur au serveur pendant l'intervalle donné ; • **Lancer le fichier exécutable**. Kaspersky Anti-Virus lance sur le serveur le fichier exécutable indiqué. Les instructions du fichier exécutable peuvent déterminer les actions qui ne seront pas exécutées par Kaspersky Anti-Virus mais par une autre application désignée. Ainsi, le fichier exécutable peut contenir les paramètres une ligne de commande qui une fois exécutée ajoute l'ordinateur infecté à la configuration du pare-feu. Vous pouvez inclure les données de l'ordinateur infectés dans le texte du fichier exécutable à l'aide des paramètres spéciaux de la ligne de commande de Kaspersky Anti-Virus : %COMPUTER_NAME%. Lors de la sélection du fichier exécutable, vous pouvez également ajouter les clés de la ligne de commande compatible avec l'application lancée depuis ce fichier.
Valeurs possibles	Si vous avez sélectionné **Interdire l'accès des ordinateurs au serveur**, définissez la durée de la période (en jours, heures ou minutes) pendant laquelle vous souhaitez bloquer l'accès des ordinateurs infectés au serveur. Si vous avez sélectionné **Lancer le fichier exécutable**, indiquez le nom du fichier exécutable et le nom complet du chemin d'accès à ce dernier ainsi que le compte utilisateur sous les privilèges duquel le fichier sera exécuté. Le fichier exécutable doit se trouver sur le disque local du serveur protégé. Le compte utilisateur sous les privilèges desquels le fichier sera exécuté doit être enregistré sur le serveur protégé ou sur le contrôleur de domaine auquel le serveur protégé appartient.
Valeur par défaut	Blocage pendant 15 minutes

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 7.2 à la page 98 ;

- Dans l'application Kaspersky Administration Kit, cf. point 20.3.1 à la page 308.

B.4.3. Liste des ordinateurs de confiance

Paramètre	Liste des ordinateurs de confiance
Description	Vous pouvez composer une liste d'ordinateurs exclus du blocage automatique, à savoir les ordinateurs du réseau local contre lesquels Kaspersky Anti-Virus n'exécutera aucune action en cas de tentative d'écriture d'un objet infecté ou suspect depuis cet ordinateur sur le serveur protégé. Si vous ajoutez à la liste un ordinateur dont l'accès au serveur est bloqué pour l'instant, il ne sera pas débloqué directement après l'enregistrement des nouveaux paramètres. Il sera débloqué uniquement à l'issue de l'intervalle de blocage ou si vous le débloquez manuellement.
Valeurs possibles	Composez la liste des ordinateurs exclus de l'interdiction en indiquant pour chacun d'entre eux son nom de réseau, l'adresse IP ou la plage d'adresses IP. Vous pouvez indiquer uniquement les noms de réseau NetBIOS des ordinateurs, vous ne pouvez pas indiquer les noms DNS.
Valeur par défaut	La liste est vide

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 7.4 à la page 101 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.3.3 à la page 311.

B.4.4. Prévention des épidémies virales

Paramètre	Prévention des épidémies virales
Description	Lorsque la fonction *Prévention des épidémies virales* est enclenchée, Kaspersky Anti-Virus augmente le niveau de protection de la tâche **Protection en temps réel des fichiers** en exécution

	dès que le nombre d'ordinateurs dont l'accès au serveur est bloqué atteint la valeur définie. Kaspersky Anti-Virus applique des paramètres de sécurité uniques, décrits au tableau 30, à toute la couverture de protection. Si la restauration du niveau de sécurité est activée, alors dès que le nombre d'ordinateurs dont l'accès est bloqué revient à la valeur définie, Kaspersky Anti-Virus rétablit les valeurs des paramètres de protection définis dans la tâche **Protection en temps réel des fichiers**. Si vous modifiez les valeurs des paramètres de sécurité décrits au tableau 30 dans la tâche **Protection en temps réel des fichiers** en exécution après l'augmentation automatique du niveau de sécurité et avant son rétablissement, alors les nouvelles valeurs ne seront pas appliquées directement mais bien lorsque Kaspersky Anti-Virus rétablira le niveau de sécurité ou lorsque vous désactiverez la prévention des épidémies virales. Les informations relatives à la modification des paramètres de sécurité sont consignées le journal d'audit système. La prévention des épidémies virales n'est pas appliquée si les valeurs des paramètres de sécurité de la tâche **Protection en temps réel des fichiers** sont définies par une stratégie de Kaspersky Administration Kit.
Valeurs possibles	Vous pouvez définir les valeurs suivantes : • Activer/désactiver la fonction *Prévention des épidémies virales* ; indiquez le nombre limite d'ordinateurs bloqués à partir duquel Kaspersky Anti-Virus renforcera le niveau de sécurité ; • Activer/désactiver le rétablissement du niveau de sécurité, indiquez le nombre d'ordinateurs à partir duquel Kaspersky Anti-Virus rétablira le niveau de sécurité.
Valeur par défaut	Désactivé Si vous activez la fonction *Prévention des épidémies virales*, alors les valeurs par défaut suivantes seront d'application : • Seuil de renforcement du niveau de sécurité : 25 ordinateurs ; • Seuil de rétablissement du niveau de sécurité : 15 ordinateurs.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 7.5 à la page 102 ;

- Dans l'application Kaspersky Administration Kit, cf. point 20.3.4 à la page 312.

Le tableau suivant reprend les valeurs des paramètres de sécurité appliqués dans la tâche **Protection en temps réel des fichiers** lorsque le nombre d'ordinateurs dont l'accès au serveur est bloqué atteint la valeur définie.

Tableau 30. Valeurs des paramètres des sécurité de la fonction *Prévention des épidémies virales*

Paramètre de sécurité	**Valeur**
Mode de protection des objets (cf. point B.3.1, p. 399)	À l'accès et à la modification
Objets à analyser (cf. point B.3.2, p. 400)	En fonction du format
Analyser uniquement les objets neufs et modifiés (cf. point B.3.3 à la page 402)	Désactivée
Actions à exécuter sur les objets infectés (cf. point B.3.5, p. 404)	Réparer, supprimer si la réparation est impossible
Actions à exécuter sur les objets suspects (cf. point B.3.6, p. 406)	Quarantaine
Traiter les objets composés (cf. point B.3.4, p. 402)	Les valeurs des paramètres suivants sont activées : • tous les archives SFX ; • tous les objets compactés ; • tous les objets OLE intégrés. Les valeurs des paramètres suivants ne changent pas : • archives ; • bases de données de messagerie ; • messages de texte plat.
Analyse des flux complémentaires du système de fichiers (NTFS) (cf. point B.3.2, p. 400)	Activé

Analyse des secteurs d'amorçage des disques et MBR (cf. point B.3.2, p. 400)	Activé
Durée maximale de l'analyse d'un objet (cf. point B.3.10, p. 413)	60 sec.
Taille maximale de l'objet composé analysé (cf. point B.3.11, p. 413)	Non installé

Les valeurs des paramètres de sécurité suivants ne changent pas :

- L'exclusion des objets (cf. point B.3.8, p. 410) ;
- L'exclusion des menaces (cf. point B.3.9, p. 411) ;
- Application de la technologie iChecker (cf. point B.3.12, p. 414) ;
- Application de la technologie iSwift (cf. point B.3.13, p. 415).

B.5. Paramètres des tâches de mise à jour

Les tâches de mise à jour de Kaspersky Anti-Virus sont définies par les paramètres suivants :

- Paramètres communs à l'ensemble des tâches de mise à jour :
  - Source des mises à jour (cf. point B.5.1, p. 423) ;
  - Mode du serveur FTP pour la connexion au serveur protégé (cf. point B.5.2, p. 424) ;
  - Délai d'attente pour la connexion à la source des mises à jour (cf. point B.5.3, p. 425) ;
  - Paramètres du serveur proxy :
    - Requête du serveur proxy pour la connexion à diverses sources de la mise à jour (cf. point B.5.4.1, p. 426) ;
    - Adresse du serveur proxy (cf. point B.5.4.2, p. 427) ;
    - Méthode de vérification de l'authenticité lors de l'accès au serveur proxy (cf. point B.5.4.3, p. 428) ;
  - Paramètres régionaux pour l'optimalisation de la réception des mises à jour (cf. point B.5.5, p. 429) ;

- Paramètres de la tâche de **Mise à jour des modules de l'application** :
  - Copie et installation des mises à jour des modules ou simple vérification de leur présence (cf. point B.5.6.1, p. 431) ;
  - Réception des informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus (cf. point B.5.6.2, p. 431) ;
- Paramètres de la tâche **Copie des mises à jour** :
  - Composition des mises à jour (cf. point B.5.7.1, p. 432) ;
  - Dossier pour l'enregistrement des mises à jour (cf. point B.5.7.2, p. 434).

B.5.1. Source des mises à jour

Paramètre	Source des mises à jour
Description	Vous pouvez sélectionner la source depuis laquelle Kaspersky Anti-Virus téléchargera les mises à jour des bases ou des modules de l'application en fonction du plan de mise à jour utilisé par votre entreprise (des exemples de schémas sont repris au point 10.3 à la page 154).
Valeurs possibles	La source des mises à jour peut être : • **Serveurs de mise a jour de Kaspersky Lab**. Kaspersky Anti-Virus télécharge les mises à jour depuis un des serveurs de mise à jour de Kaspersky Lab situés dans divers pays. Les mises à jour sont téléchargées selon le protocole HTTP ou FTP. • **Kaspersky Administration Server**. Vous pouvez sélectionner cette source si vous utilisez l'application Kaspersky Administration Kit pour l'administration centralisée de la protection antivirus des ordinateurs de votre entreprise. Kaspersky Anti-Virus copiera la mise à jour sur le serveur protégé depuis le serveur d'administration Kaspersky Administration Kit installé dans le réseau local. • **Serveurs HTTP, FTP ou dossiers réseau personnalisés**. Kaspersky Anti-Virus copiera la mise à jour depuis la source que vous aurez définie : dossier FTP, serveur HTTP ou un ordinateur quelconque du réseau local. Vous pouvez définir une ou plusieurs sources de mises à jour. Kaspersky Anti-Virus contactera chaque source indiquée dans l'ordre si la source

	précédente n'est pas disponible. Vous pouvez définir l'ordre dans lequel Kaspersky Anti-Virus va contacter les sources, activer ou désactiver l'utilisation de sources distinctes. Vous pouvez configurer l'organisation des requêtes de Kaspersky Anti-Virus aux serveurs de mise à jour de Kaspersky Lab au cas où les sources définies par l'utilisateur ne serait pas accessibles. **Remarque** Vous pouvez utiliser des variables dans le chemin. Si vous utilisez les variables, définir l'utilisateur pour exécuter la tâche (cf. point 5.9 p. 65). Vous ne pouvez pas sélectionner des dossiers sur des disques de réseaux connectés en guise de sources de mise à jour.
Valeur par défaut	Vous pouvez consulter la liste des serveurs de mise à jour de Kaspersky Lab dans le fichier %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.2. Mode du serveur FTP pour la connexion au serveur protégé

Paramètre	Mode du serveur FTP pour la connexion au serveur protégé (**Utiliser le FTP en mode passif si possible**)
Description	La connexion aux serveurs de mises à jour selon le protocole FTP s'opère selon le mode FTP passif : on suppose que le réseau local de l'entreprise utilise un pare-feu. Quand le mode passif du serveur FTP ne fonctionne pas, le mode actif est enclenché automatiquement
Valeurs possibles	Sélectionnez le mode du serveur FTP : activez ou désactivez l'utilisation du mode passif du FTP

Valeur par défaut	Mode FTP passif, si possible

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.3. Délai d'attente lors de la connexion à la source des mises à jour

Paramètre	Délai d'attente lors de la connexion (**Délai d'attente**)
Description	Ce paramètre définit le délai d'attente lors de la connexion à la source des mises à jour
Valeurs possibles	Définissez le délai d'attente en secondes
Valeur par défaut	10 s

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.4. Utilisation et paramètres du serveur proxy

Kaspersky Anti-Virus adopte les paramètres suivants pour l'accès au serveur proxy :

- Requête adressée au serveur proxy lors de la connexion à diverses sources de mises à jour (cf. point B.5.4.1, p. 426) ;

- Paramètres du serveur proxy (cf. point B.5.4.2, p. 427) ;
- Méthode de vérification de l'authenticité lors de l'accès au serveur proxy (cf. point B.5.4.3, p. 428).

B.5.4.1. Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour

Paramètre	Requête adressée au serveur proxy lors de la connexion aux sources des mises à jour.
Description	Par défaut, lors de la connexion aux serveurs de mise à jour de Kaspersky Lab, Kaspersky Anti-Virus contacte le serveur proxy du réseau et lors de la connexion aux sources de mise à jour définies par l'utilisateur (serveurs HTTP ou FTP ou ordinateurs définis), il contourne le serveur proxy : il suppose que ces sources se trouvent dans le réseau local. N'oubliez pas que les extensions des fichiers des mises à jour des bases sont aléatoires. Si le serveur proxy de votre réseau possède une règle d'interdiction pour le téléchargement de fichiers possédant une certaine extension, il est alors conseillé d'autoriser le téléchargement de fichier de n'importe quelle extension depuis les serveurs de mises à jour de Kaspersky Lab. Vous pouvez consulter la liste des serveurs de mises à jour de Kaspersky Lab dans le fichier %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\updcfg.xml.

Valeurs possibles	• Si en qualité de source des mises à jour vous avez désigné un serveur de mises à jour de Kaspersky Lab, alors assurez-vous que la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab** est cochée. • Si la connexion à un des serveurs FTP ou HTTP défini par l'utilisateur requiert un accès au serveur proxy, cochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs personnalisés**. Après avoir coché cette case, vous pouvez désactiver l'envoi de requête au serveur proxy pour accéder aux autres sources de mise à jour pour lesquelles ces requêtes ne sont pas nécessaires (par exemple, s'il s'agit d'ordinateurs du réseau local) : cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.
Valeur par défaut	Kaspersky Anti-Virus contacte le serveur proxy uniquement lors de la connexion aux serveurs de mises à jour HTTP ou FTP de Kaspersky Lab.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.4.2. Paramètres du serveur proxy

Paramètre	Paramètres du serveur proxy
Description	Lors de la connexion aux serveurs de mise à jour FTP ou HTTP Kaspersky Anti-Virus identifie par défaut les paramètres du serveur proxy utilisé sur le réseau local grâce au protocole Web Proxy Auto-Discovery Protocol (WPAD). Vous pouvez indiquer manuellement les paramètres du serveur proxy, par exemple si le protocole WPAD n'est pas configuré dans votre réseau local.
Valeurs possibles	Indiquez l'adresse IP ou le nom DNS du serveur (par exemple, proxy.mycompany.com) et son port. Désactivez l'utilisation du serveur proxy si le serveur FTP ou HTTP défini par l'utilisateur se trouve dans votre réseau local.

Valeur par défaut	Identifier automatiquement les paramètres du serveur proxy

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.4.3. Méthode de vérification de l'authenticité lors de l'accès au serveur proxy

Paramètre	Méthode de vérification de l'authenticité lors de l'accès au serveur proxy.
Description	Ce paramètre définit la méthode de vérification de l'authenticité de l'utilisateur lors de l'accès au serveur proxy utilisé lors de la connexion aux serveurs FTP ou HTTP de mises à jour.
Valeurs possibles	Choisissez une des valeurs suivantes : • **Aucune authentification requise**. Sélectionnez cette option si l'accès au serveur proxy ne requiert pas la vérification de l'authenticité. • **Utiliser l'authentification NTLM**. Kaspersky Anti-Virus utilisera le compte utilisateur indiqué dans la tâche pour accéder au serveur proxy. (Si le paramètre **Lancer sous** ne définit aucun autre compte utilisateur, alors la tâche sera exécutée sous le compte **Système local** (**SYSTEM**). Vous pouvez sélectionner cette méthode si le serveur proxy prend en charge la vérification intégrée de l'authenticité Microsoft Windows (NTLM authentification) (pour en savoir plus sur l'utilisation des comptes utilisateur pour l'exécution des tâches, lisez le point 5.9.1 à la page 65). • **Utiliser l'authentification NTLM avec utilisateur et mot de passe**. Kaspersky Anti-Virus utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy. Vous pouvez sélectionner cette méthode si le serveur proxy est compatible avec la fonction intégrée de vérification de l'authenticité de Microsoft Windows. Saisissez le nom d'utilisateur et le mot de passe ou sélection-

	nez un utilisateur dans la liste. • **Utiliser le nom d'utilisateur et le mot de passe**. Vous pouvez sélectionner la vérification traditionnelle de l'authenticité (Basic authentification). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste. Vous pouvez sélectionner cette méthode si, par exemple, le compte utilisateur avec les privilèges duquel la tâche de mise à jour sera exécutée ne jouit pas des privilèges d'accès au serveur proxy et que vous souhaitez utiliser un autre compte utilisateur. Si la vérification traditionnelle de l'authenticité en fonction du nom et du mot de passe de l'utilisateur échoue, Kaspersky Anti-Virus utilisera la vérification intégrée de l'authenticité de Microsoft Windows selon le compte utilisateur utilisé dans la tâche.
Valeur par défaut	La vérification de l'authenticité lors de l'accès au serveur proxy n'est pas réalisée.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.5. Paramètres régionaux pour l'optimalisation de la réception des mises à jour (Emplacement)

Paramètre	Paramètres régionaux pour l'optimalisation de la réception des mises à jour (**Emplacement**).
Description	Les serveurs de mises à jour de Kaspersky Lab se trouvent dans divers pays. Grâce à ce paramètre, vous pouvez indiquer le pays où se trouve le serveur à protéger. Kaspersky Anti-Virus optimalise le téléchargement des mises à jour sur le serveur depuis les serveurs de mises à jour de Kaspersky Lab en sélectionnant le plus proche.

Valeurs possibles	Vous pouvez sélectionner le pays où se trouve le serveur à protéger.
Valeur par défaut	Kaspersky Anti-Virus identifie par défaut le pays où se trouve le serveur à protéger sur la base des paramètres régionaux définis dans Microsoft Windows, pour Microsoft Windows Server 2003, selon la valeur de la variable **Location**, définie pour l'utilisateur par défaut (Default User). Par exemple, si dans les paramètres régionaux de Microsoft Windows vous (pour l'utilisateur courant) attribuez la valeur **Russie** à la variable Location, alors elle demeurera pour l'utilisateur par défaut. Pour optimiser la demand pour les mises à jour vous pouvez faire l'un de cettes actions : • dans les paramètres régionaux de Microsoft Windows vous identifie la location de la variable **Location**, définie pour l'utilisateur par défaut (Default User) ; • dans Anti-Virus exécuter la tâche de mises à jour pour l'utilisateur courant ; • identifie par défaut le pays de serveur, définie avec l'aide de paramètre de mises à jour **Location du serveur à protéger**.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.1 à la page 160 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.6. Paramètres de la tâche de *Mise à jour des modules de l'application*

La tâche **Mise à jour des modules de l'application** accepte les paramètres suivants :

- Copie et installation des mises à jour critiques des modules ou simple vérification de leur présence (cf. point B.5.6.1, p. 431) ;

- Réception des informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus (cf. point B.5.6.2, p. 431).

B.5.6.1. Copie et installation des mises à jour critiques ou simple vérification de leur présence

Paramètre	Copie et installation des mises à jour critique ou simple vérification de leur présence
Description	A l'aide des paramètres de la tâche **Mise à jour des modules de l'application**, vous pouvez décider de télécharger et d'installer immédiatement les mises à jour critiques des modules de l'application ou de vérifier uniquement si elles sont disponibles.
Valeurs possibles	Choisissez une des valeurs suivantes : • **Rechercher uniquement la présence des mises à jour critiques des modules de l'application**. Vous pouvez choisir cette option, par exemple, pour savoir si des mises à jour urgentes des modules de Kaspersky Anti-Virus ont été diffusées. • **Copier et installer les mises à jour critiques des modules de l'application**.
Valeur par défaut	**Rechercher uniquement la présence des mises à jour critiques des modules de l'application**

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.2 à la page 165 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.6.2. Obtention d'informations sur la diffusion des mises à jour prévues des modules de Kaspersky Anti-Virus

Paramètre	Obtention d'informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus

Description	Vous pouvez obtenir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus. Pour être alerté de la diffusion des mises à jour prévue, définissez la valeur **Recevoir des informations sur les mises à jour des modules de l'application prévues** et configurez la notification pour l'événement « Des mises à jour des modules d'application sont disponibles » de Kaspersky Anti-Virus qui contiendra le lien vers la page de notre site d'où vous pourrez télécharger les mises à jour prévues (pour en savoir plus sur la configuration des notification, consultez le point 15.2 à la page 238).
Valeurs possibles	Recevoir/ne pas recevoir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus
Valeur par défaut	**Obtenir des informations sur les mises à jour prévues disponibles des modules de Kaspersky Anti-Virus**

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.2 à la page 165 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.7. Paramètres de la tâche *Copie des mises à jour*

La tâche **Copie des mises à jour** de Kaspersky Anti-Virus accepte les paramètres suivants :

- Composition des mises à jour de la tâche **Copie des mises à jour** (B.5.7.1 p. 432) ;
- Dossier pour l'enregistrement des mises à jour (B.5.7.2, p. 434).

B.5.7.1. Composition des mises à jour

Paramètre	Composition des mises à jour
Description	Ce paramètre vous permet de définir la composition des mises à jour copiées. Vous pouvez copier uniquement les mises à jour des bases de Kaspersky Anti-Virus, uniquement les mises à jour

	urgentes des modules ou toutes les mises à jour disponibles Ou vous pouvez copier les mises à jour des bases et des modules non seulement pour Kaspersky Anti-Virus mais également pour les autres applications de la version 6.0 de Kaspersky Lab puis, répartir ces mises à jour vers d'autres ordinateurs du réseau local où les logiciels antivirus de Kaspersky Lab de cette version sont installés. Kaspersky Anti-Virus enregistre par défaut les fichiers des mises à jour dans le répertoire %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\UpdateDistribution\.
Valeurs possibles	Choisissez une des valeurs suivantes : • Pour télécharger et enregistrer uniquement la mise à jour des bases dans le répertoire indiqué, sélectionnez **Copier les mises à jour des bases de l'application** ; • Pour télécharger et enregistrer uniquement la mise à jour des modules de l'application dans le répertoire indiqué, sélectionnez **Copier les mises à jour critiques des modules de l'application** ; • Pour télécharger et enregistrer uniquement la mise à jour des bases et celles des modules de l'application dans le répertoire indiqué, sélectionnez **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application** ; Pour obtenir les mises à jour des bases et des modules non seulement pour Kaspersky Anti-Virus mais pour les autres applications de Kaspersky Lab de la version 6.0 ou suivante, sélectionnez **Copier les mises à jour des bases et des modules pour toutes les applications de Kaspersky Lab de la version 6.0 ou suivante**.
Valeur par défaut	Kaspersky Anti-Virus copie uniquement les mises à jour des bases de Kaspersky Anti-Virus.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.3 à la page 167 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.5.7.2. Dossier pour l'enregistrement des mises à jour

Paramètre	Dossier pour l'enregistrement des mises à jour
Description	Ce paramètre vous permet d'indiquer le répertoire dans lequel les fichiers des mises à jour seront enregistrés
Valeurs possibles	Indiquez le répertoire local ou de réseau dans lequel Kaspersky Anti-Virus enregistrera les mises à jour copiées. Pour définir un répertoire de réseau, saisissez son nom et son chemin d'accès au format UNC (Universal Naming Convention). Vous ne pouvez pas désigner des répertoires sur des disques de réseau connectés, ni sur des disques créés à l'aide de la commande SUBST. Vous pouvez utiliser des variables dans le chemin. Si vous utilisez les variables, définir l'utilisateur pour exécuter la tâche (cf. point 5.9 à la page 65). Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via MMC, installé sur le poste de travail distant de l'administrateur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Update\Distribution\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.3 à la page 167 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.6. Paramètres de quarantaine

La quarantaine possède les paramètres suivants :

- Répertoire de quarantaine (cf. point B.6.1, p. 435) ;
- Taille maximale de la quarantaine (cf. point B.6.2, p. 435) ;
- Seuil d'espace libre dans la quarantaine (cf. point B.6.3, p. 436) ;
- Restaurer dans le dossier (cf. point B.6.4, p. 437).

B.6.1. Répertoire de quarantaine

Paramètre	Répertoire de quarantaine
Description	Vous pouvez utiliser un répertoire de quarantaine différent du répertoire de quarantaine installé par défaut.
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Kaspersky Anti-Virus commencera à placer les objets dans le répertoire indiqué par le paramètre dès que vous aurez enregistré la nouvelle valeur du paramètre. Si le répertoire indiqué n'existe pas ou est inaccessible, Kaspersky Anti-Virus utiliser le répertoire défini par défaut. Pour indiquer le chemin d'accès au répertoire de quarantaine, vous pouvez utiliser des variables. Dans le cluster, les répertoires de disque de quorum ou de cluster ne peuvent être des répertoires de quarantaine.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Quarantine\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 10.5.3 à la page 167 ;
- Dans l'application Kaspersky Administration Kit, cf. point 21.2 à la page 335.

B.6.2. Taille maximale de la quarantaine

Paramètre	Taille maximale de la quarantaine
Description	Ce paramètre définit la taille maximale de la quarantaine, à savoir le volume total de données dans le dossier de quarantaine. Le paramètre **Taille maximale de la quarantaine** est informatif. Il ne limite pas la taille de la quarantaine et constitue simplement un critère d'enregistrement des événements qui permet à l'administrateur de surveiller l'état du dossier. Une fois que la taille maximale a été atteinte, Kaspersky Anti-Virus continue à placer les objets suspects en quarantaine. Vous pouvez configurer la notification sur le dépassement de la taille maximale de la quarantaine. Kaspersky Anti-Virus enverra le message dès que le volume totale des données en quarantaine atteindra la valeur indiquée (pour en savoir plus sur les notifications, lisez le Chapitre 15 à la page 236. La valeur recommandée est égale à 200 Mo.
Valeurs possibles	1 à 999 Mo
Valeur par défaut	Non installé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 11.8 à la page 186 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.4.2 à la page 318.

B.6.3. Seuil d'espace libre dans la quarantaine

Paramètre	Seuil d'espace libre dans la quarantaine
Description	Ce paramètre est utilisé conjointement au paramètre **Taille maximale de la quarantaine**. Le paramètre **Seuil d'espace libre dans la quarantaine** est informative. Il ne limite pas la taille du dossier de quarantaine

	mais permet d'obtenir des informations sur la proximité du remplissage de la quarantaine. Si le volume d'espace disponible dans la quarantaine est inférieur à la valeur du seuil, Kaspersky Anti-Virus enregistre l'événement **Le seuil d'espace disponible dans la quarantaine est dépassé** et continue à isoler les objets suspects. Vous pouvez configurer les notifications pour l'événement **Le seuil d'espace libre de la quarantaine est dépassé** (les informations sur la configuration des notifications sont reprises au Chapitre 15 à la page 236).
Valeurs possibles	Indiquez le volume en Mo ; il doit être inférieur à la valeur définie par le paramètre **Taille maximale de la quarantaine**. La valeur recommandée est égale à 50 Mo
Valeur par défaut	Non installé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 11.8 à la page 186 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.4.2 à la page 318.

B.6.4. Restaurer dans le dossier

Paramètre	Restaurer dans le dossier
Description	Le paramètre définit le répertoire spécial utilisé pour les objets restaurés sur le serveur protégé. Lors de la restauration d'un objet, vous pouvez sélectionner l'emplacement où l'objet restauré sera conservé : dans le répertoire d'origine, dans un dossier spécial pour les objets restaurés sur le serveur protégé ou dans un autre dossier indiqué (sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou dans un répertoire de réseau).
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via MMC, installé sur le poste de travail distant de l'administra-

	teur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur. Vous pouvez utiliser des variables de système pour specifier les objets restaurés ; vous ne pouvez pas utiliser des variables d'utilisateur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Restored\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 11.8 à la page 186 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.4.2 à la page 318.

B.7. Paramètres de sauvegarde

La sauvegarde possède les paramètres suivants :

- Dossier de sauvegarde (cf. point B.7.1, p. 438) ;
- Taille maximale du dossier de sauvegarde (cf. point B.7.2, p. 439) ;
- Seuil d'espace libre dans la sauvegarde (cf. point B.7.3, p. 440) ;
- Restaurer dans le dossier (cf. point B.7.4, p. 441).

B.7.1. Dossier de sauvegarde

Paramètre	Dossier de sauvegarde
Description	Vous pouvez utiliser un répertoire de sauvegarde différent du répertoire de sauvegarde installé par défaut
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet). Kaspersky Anti-Virus utilise directement le répertoire indiqué dès que la nouvelle valeur

	du paramètre a été enregistrée. Si le répertoire indiqué n'existe pas ou est inaccessible, Kaspersky Anti-Virus utiliser le répertoire défini par défaut. Pour indiquer le chemin d'accès au répertoire de sauvegarde, vous pouvez utiliser des variables. Dans un cluster, les répertoires de disque de quorum ou des clusters ne peuvent être des dossiers de sauvegarde. Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via MMC, installé sur le poste de travail distant de l'administrateur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur.
Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Backup\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 12.5 à la page 200 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.5.2 à la page 321.

B.7.2. Taille max. du dossier de sauvegarde

Paramètre	Taille max. du dossier de sauvegarde
Description	Ce paramètre définit la taille maximale de la sauvegarde, à savoir le volume total de données dans le dossier de sauvegarde. Le paramètre **Taille maximale du dossier de sauvegarde** est informatif. Il ne limite pas la taille de la sauvegarde et constitue simplement un critère d'enregistrement des événements qui permet à l'administrateur de surveiller l'état du dossier. Une fois que la taille maximale a été atteinte, Kaspersky Anti-Virus continue à

	placer des copies des objets infectés dans la quarantaine. Vous pouvez configurer la notification de l'administrateur sur le dépassement de la taille maximale de la sauvegarde. Kaspersky Anti-Virus enverra le message dès que le volume totale des données en sauvegarde atteindra la valeur indiquée (pour en savoir plus sur les notifications, lisez le Chapitre 15 à la page 236). La valeur recommandée est égale à 200 Mo
Valeurs possibles	1 à 999 Mo
Valeur par défaut	Non installé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 12.5 à la page 200 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.5.2 à la page 321.

B.7.3. Seuil d'espace libre de la sauvegarde

Paramètre	Seuil d'espace libre
Description	Ce paramètre est utilisé conjointement au paramètre **Taille maximale du dossier de sauvegarde**. Ce paramètre est informatif. Il ne limite pas la taille du dossier de de sauvegarde mais permet d'obtenir des informations sur la proximité de son remplissage. Si le volume d'espace disponible dans la sauvegarde est inférieur à la valeur du seuil, Kaspersky Anti-Virus enregistre l'événement **Le seuil d'espace disponible dans la sauvegarde est dépassé** et continue à isoler les objets suspects. Vous pouvez configurer les notifications pour les événements de ce type (les informations sur la configuration des notifications sont reprises au Chapitre 15 à la page 236).

Valeurs possibles	Indiquez le volume en Mo ; il doit être inférieur à la valeur définie par le paramètre **Taille maximale de la sauvegarde**. La valeur recommandée est égale à 50 Mo
Valeur par défaut	Non installé

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 12.5 à la page 200 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.5.2 à la page 321.

B.7.4. Restaurer dans le dossier

Paramètre	Restaurer dans le dossier
Description	Le paramètre définit le répertoire spécial utilisé pour les objets restaurés sur le disque local du serveur protégé. Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où le fichier restauré sera conservé : dans le répertoire d'origine, dans un dossier spécial pour les objets restaurés sur le serveur protégé ou dans un autre dossier indiqué (sur l'ordinateur où la console de Kaspersky Anti-Virus est installée ou dans un répertoire de réseau). Si vous administrez Kaspersky Anti-Virus sur le serveur protégé via MMC, installé sur le poste de travail distant de l'administrateur, vous devez entrer dans le groupe des administrateurs locaux sur le serveur protégé afin de consulter les dossiers du serveur.
Valeurs possibles	Indiquez le répertoire sur le disque local du serveur protégé (nom du répertoire ou chemin d'accès complet).

Valeur par défaut	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\ Restored\ Vous pouvez utiliser la variable de Kaspersky Anti-Virus %KAVWSEEAPPDATA% afin de désigner le répertoire de Kaspersky Anti-Virus %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\.

Pour savoir comment configurer ce paramètre :

- Dans la console de Kaspersky Anti-Virus dans MMC, cf. point 12.5 à la page 200 ;
- Dans l'application Kaspersky Administration Kit, cf. point 20.5.2 à la page 321.

ANNEXE C. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

C.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la “météo” des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d’informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la zone de notification de la barre des tâches ;
- S’abonner et se désabonner aux canaux d’information de Kaspersky Lab ;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d’informations non lues ;
- Lire les informations dans les canaux auxquels on est abonné ;
- Consulter la liste des canaux et leur contenu ;
- Ouvrir dans le navigateur une page contenant la version complète de l’information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s’agit d’un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l’ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l’analyse, l’utilisateur peut :

- Exclure les archives et les bases de données de messagerie ;
- Sélectionner les bases standard ou étendues ;

- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie ;
- Sélectionner les bases standard ou étendues ;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.

- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.
- **Le contrôle des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique**. Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.
- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!.
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers** : n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont:

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel :** tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;

- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;
- **Protection contre les sms et mms indésirables .**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur ;
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;

- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;
- *Génération de rapports détaillés* ;
- *Mise à jour automatique des bases* de l'application.

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable ;
- Défense proactive contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;
- Annulation des modifications malveillantes dans le système ;
- Protection contre les tentatives d'hameçonnage et le courrier indésirable ;
- Redistribution dynamique des ressources lors de l'analyse complète du système ;
- Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;
- Compatibilité avec Cisco® NAC (Network Admission Control) ;

- Analyse du courrier électronique et du trafic Internet en temps réel ;
- Blocage des fenêtres pop up et des bannières publicitaires pendant la navigation sur Internet ;
- Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;
- Outils de création d'un disque de démarrage capable de restaurer le système après une attaque de virus ;
- Système développé de rapports sur l'état de la protection ;
- Mise à jour automatique des bases ;
- Compatibilité absolue avec les systèmes d'exploitation 64 bits ;
- Optimisation du fonctionnement de l'application sur les ordinateurs portables (technologie Intel® Centrino® Duo pour ordinateurs portables) ;
- Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Répartition de la charge entre les processeurs du serveur* ;
- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;

- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases*.

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers ;
- Protection des serveurs de messagerie Sendmail, Qmail, Posftix et Exim ;
- Analyse de tous les messages sur le serveur Microsoft Exchange y compris les dossiers partagés ;
- Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino ;
- Protection contre les tentatives d'hameçonnage et le courrier indésirable ;
- Prévention des épidémies de virus et des diffusions massives ;
- Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;
- Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;
- Compatibilité avec Cisco® NAC (Network Admission Control) ;

- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;
- Utilisation sécurisée des réseaux sans fil Wi-Fi ;
- Analyse du trafic Internet en temps réel ;
- Annulation des modifications malveillantes dans le système ;
- Redistribution dynamique des ressources lors de l'analyse complète du système ;
- Isolement des objets suspects dans un répertoire spécial ;
- Système de rapports sur l'état de la protection ;
- Mise à jour automatique des bases.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;

- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™) ;
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.

- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Filtrage des messages non sollicités* ;
- *Analyse des messages et des pièces jointes du courrier entrant et sortant* ;
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Filtrage des messages* en fonction du type de pièce jointe ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* du logiciel ;
- *Prévention des épidémies de virus* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Système de rapports* sur l'activité de l'application ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Analyse du trafic Internet* (HTTP/FTP) en temps réel ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* ;
- *Système de rapports sur le fonctionnement de l'application* ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

C.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://kb.kaspersky.fr/faq.php
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://kb.kaspersky.fr E-mail : info@fr.kaspersky.com

INDEX

A l’accès, 399
A l’accès et en cas de modification, 399
A l’exécution, 399
A partir du, 393
A propos du programme, 37
Accès au service d'administration de Kaspersky Anti-Virus, 30
Accès aux applications COM, 33
Accès aux fonctions de Kaspersky Anti-Virus, 38
Action à exécuter sur les objets infectés dans la tâche, 404
Action à exécuter sur les objets infectés dans les tâches d’analyse à la demande, 405
Action à exécuter sur les objets suspects dans la tâche, 406
Actions à exécuter sur les objets en fonction de la catégorie de menace, 408
Activation et désactivation de la création d'un vidage, 267
Activation et désactivation de la programmation, 64
Activation ou désactivation de l'interdiction automatique d'accès des ordinateurs, 98
Activation, configuration et désactivation de la constitution d'un journal de traçage, 265
Administration de Kaspersky Anti-Virus via la ligne de commande, 247
Administration de l’état des tâches, 40
Administration de la tâche indiquée en mode asynchrone, 256
Adware, 19
Affichage de l'aide sur les commandes de Kaspersky Anti-Virus, 249
Afficher l'icône de Kaspersky Anti-Virus, 37
Ajout et suppression d'une clé, 264
Analyse à la demande, 15
Analyse au démarrage du système, 121
Analyse des objets en quarantaine, 121
Analyse des objets en quarantaine. Paramètres de la tâche *Analyse de la quarantaine*, 177
Analyse du secteur indiqué, 250
Analyser les flux NTFS alternatifs, 400
Analyser mon ordinateur, 121
Application de la barre des tâches, 37
Application de la technologie iChecker™, 414
Application de la technologie iSwift™, 415
Archives, 403
Archives autoextractibles, 403
Arrêt de la tâche, 60
Arrêt du service de Kaspersky Anti-Virus, 44
Autorisations, 41
Autorisations spéciales, 43
Autres programmes malveillants, 19
Bases, 20
Bases de données de messagerie, 403
Bloquer l’accès + réparer, 404
Cacher l'icône de Kaspersky Anti-Virus, 37
Code de retour, 270

Codes des sous-systèmes pouvant être ajoutés au journal de traçage, 389
Compte Système local (SYSTEM), 65
Compte utilisateur pour l'exécution des tâches, 65
Configuration de la quarantaine, 186
Configuration des notifications, 236
Configuration des paramètres de blocage automatique de l'accès depuis les ordinateurs, 416
Configuration des paramètres de la sauvegarde, 200
Configuration des paramètres de la tâche *Copie des mises à jour*, 167
Configuration des paramètres de la tâche *Mise à jour des modules de l'application*, 165
Configuration des paramètres de protection, 79
Configuration des tâches d'analyse à la demande, 122
Configuration des tâches liées à la mise à jour, 422
Configuration manuelle des paramètres de sécurité, 136
Consignation des événements, 204
Consigner les informations de débogage dans le fichier, 385
Console de Kaspersky Anti-Virus, 35, 37, 38
Console de Kaspersky Anti-Virus dans MMC, 28
Constitution d'un journal de traçage, 385, 387
Constitution d'une couverture de l'analyse dans les tâches d'analyse à la demande, 125
Constitution d'une couverture de protection dans la tâche *Protection en temps réel des fichiers*, 72
Consultation des statistiques, 40
Consultation des statistiques d'interdiction, 107
Consultation du rapport détaillé sur les événements dans la tâche, 211
Création de fichiers de vidage de la mémoire des processus de Kaspersky Anti-Virus, 390
Date d'entrée en vigueur de la planification, 393
Date finale de planification, 394
Dossier des fichiers de débogage, 386
Dossier pour la restauration des objets, 437
Durée de conservation des rapports, 381
Durée de conservation du journal d'audit système, 382
Durée maximale de l'analyse d'un objet, 413
Emplacement de la quarantaine, 435
Enregistrement des paramètres, 58
Enregistrement des valeurs des paramètres dans un modèle. Application du modèle, 140
Enregistrement d'une tâche après modification de ses paramètres, 58
Enregistrer les événements, 228
Envoi des objets suspects à Kaspersky Lab pour examen, 184
Evénement dans les rapports et le journal des événements, 217
Exclusion des menaces, 411
Exclusion des objets, 410
exportation des paramètres, 50
Fenêtre des services des terminaux, 237
Filtrage des événements dans le journal d'audit système, 222
Filtrage des objets en quarantaine, 175
Fréquence d'exécution, 392

Gestion de la quarantaine et de la sauvegarde, 40
Gestion des clés de licence, 41
Gestion des rapports, 40
Gestion des tâches, 40
Heure de la première exécution de la tâche, 393
Icône de Kaspersky Anti-Virus dans la barre des tâches
couleur, noir et blanc, 36
importation des paramètres, 50
Inclusion des chemins de réseau dans la couverture d'analyse, 129
Inclusion des disques, répertoires et fichiers dynamiques dans la couverture de protection, 76
Interaction avec l'utilisateur, 385
Interaction avec l'utilisateur, 387, 388
Interdiction de l'accès des ordinateurs, 97
Interdiction manuelle de l'accès des ordinateurs, 105
Interdire l'accès, 404
Interdire l'accès + exécuter l'action recommandée, 404
Interdire l'accès + réparer, supprimer si la réparation est impossible, 404
Interdire l'accès + supprimer, 404
Isolement des objets suspects, 171
Journal d'audit système, 219
JScript, 16
Kaspersky Administration Server, 423
KAVSHELL DUMP, 267
KAVSHELL FULLSCAN, 255
KAVSHELL HELP, 249
KAVSHELL LICENSE, 264
KAVSHELL ROLLBACK, 264
KAVSHELL RTP, 258
KAVSHELL SCAN, 250
KAVSHELL START, 249
KAVSHELL STOP, 249
KAVSHELL TASK, 256
KAVSHELL TRACE, 265
KAVSHELL UPDATE, 258
KAVWSEE Administrators, 30
L'analyse complète de l'ordinateur n'a pas été réalisée depuis longtemps, 384
La base de données est dépassée, 384
La base de données est périmée, 384
Lancement de la console de Kaspersky Anti-Virus depuis le menu *Démarrer*, 35
Lancement de la tâche *Analyse du poste de travail*, 255
Lancement de la tâche de mise à jour des bases de Kaspersky Anti-Virus, 258
Lancement des tâches non exécutées, 396
Lancement du fichier exécutable, 237
Lancement du service de Kaspersky Anti-Virus, 44
Lancement d'une tâche, 60
Lancement et arrêt de Kaspersky Anti-Virus, 249
Lancement ou arrêt des tâches de protection en temps réel, 258
Lancer comme, 66
Lecture des paramètres, 40
Lecture des privilèges, 41
Lecture des rapports, 40
Levée de l'interdiction de l'accès de l'ordinateur, 107
Logiciels publicitaires, 19
Malware, 19
Message de texte plat, 403
Mises à jour, 37
Mode de protection, 399
Mode intelligent, 399
Modification des paramètres, 40
Modification des privilèges, 39, 41
Modifier les privilèges des utilisateurs, 41
Ne pas conserver les événements plus de … jours, 382

Ne pas conserver les rapports et les événements plus de, 47
Ne pas conserver les rapports et les événements plus de ... jours, 47
Ne pas conserver les rapports plus de … jours, 381
Ne pas exécuter la récupération automatique plus de … fois, 380
Niveau de protection Protection maximum, 80
Niveau de protection Recommandé, 79
Niveau de protection Vitesse maximale, 79
Niveaux de sécurité prédéfinis dans la tâche *Protection en temps réel des fichiers*, 79
Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan, 379
Nombre de processus actifs pour les tâches d'analyse à la demande en arrière-plan, 46
Nombre de processus de travail utilisés par les tâches de protection en temps réel, 378
Nombre de processus pour la protection en temps réel, 46
Nombre maximum de processus actifs, 46
Nombre maximum de processus de travail, 377
Notification par courrier électronique, 238
Notification via le service de messagerie de Microsoft Windows, 237
Notifications Services de messagerie Microsoft Windows, 237
Nouvelle tâche, 56
Objets à analyser, 400
Objets analysés en fonction d'une liste d'extensions, 400
Objets analysés en fonction de masques d'extension, 400
Objets analysés en fonction du format, 400
Objets compactés, 403
Objets infectés, 20
Objets OLE intégrés, 403
Objets présentant un risque potentiel, 21
Objets suspects, 20
Panneau des tâches, 38
Paramètres de quarantaine par défaut, 434
Paramètres de sauvegarde par défaut, 438
Paramètres de sécurité
  Application du modèle, 86, 87, 140, 141
  Configuration manuelle des paramètres de sécurité, 82
Paramètres généraux de Kaspersky Anti-Virus, 45
Pornware, 19
Port TCP 135, 33
Pose à partir de…jusqu'à, 396
Présentation de la mise à jour des bases de Kaspersky Anti-Virus, 152
Présentation de la mise à jour des modules logiciels, 153
Programmation d'une tâche, 60
Protection en temps réel des fichiers, 15, 68
Rapports sur l'exécution des tâches, 205
Recherche de fichiers dans la sauvegarde, 194
Règle d'exclusion, 110
Remise à l'état antérieur à la mise à jour des bases, 170
Remise à l'état antérieur à la mise à jour des bases de Kaspersky Anti-Virus (ligne de commande), 264
Remise à l'état antérieur à la mise à jour des modules logiciels, 170

Renommer, 59
Répartition des heures de lancement, 392, 397
Restauration des fichiers depuis la sauvegarde, 196
Restauration des objets de la quarantaine, 179
Rétablissement de la tâche, 60
Sauvegarde des objets avant la réparation / la suppression, 190
Scripts suspects
  Autorisation et interdiction de l'exécution, 94
Se connecter à un autre ordinateur, 36
Secteurs d'amorçage et partition MBR, 400
Sélection des niveaux de sécurité prédéfinis, 132
serveurs de mises à jour de Kaspersky Lab, 423
Service d'assistance technique, 456
Service de Kaspersky Anti-Virus, 44
Seuil de déclenchement des événements, 383
sources de mise à jour définies par l'utilisateur, 423
Statistiques de Kaspersky Anti-Virus, 224
Statistiques de la tâche *Analyse des scripts*, 95
Statistiques de la tâche Protection en temps réel des fichiers, 92
Statistiques de quarantaine, 188
Statistiques de sauvegarde, 202
Statistiques des tâches, 64
Statistiques des tâches d'analyse à la demande, 147
Statistiques des tâches de mise à jour, 169
Suppression des événements du journal d'audit système, 223
Suppression des fichiers depuis la sauvegarde, 200
Suppression des objets de la quarantaine, 184
Suppression des rapports, 216
Supprimer tâche, 59
Suspension de la tâche, 60
Tâche *Protection en temps réel des fichiers*, 69
taches
  administration, 54
Tâches d'analyse à la demande, 121
Tâches de groupe, 55
Tâches de mise à jour, 158
Tâches de protection en temps réel, 68
Tâches définies par l'utilisateur, 55
Tâches locales, 54
Tâches prédéfinies, 55
Taille maximale de la quarantaine, 436
Taille maximale de l'objet composé à analyser, 413
Taille minimale de l'espace libre dans la quarantaine, 436
Téléchargement des mises à jour via le serveur d'administration Kaspersky Administration Kit, 156
Téléchargement des mises à jour via un ordinateur intermédiaire, 155
Téléchargement direct des mises à jour depuis Internet sur le serveur protégé, 155
Tous les objets, 400
Traçage pour les sous-systèmes de Kaspersky Anti-Virus, 388
Traiter les objets composés, 402
Tri des événements dans le journal d'audit système, 221
Tri des fichiers de la sauvegarde, 194
Tri des objets en quarantaine, 175
Tri des rapports, 210
Trojans, 18
Types de menaces, 16
Types de tâches, 54
Utilisation de la quarantaine, 172
Utilisation de la sauvegarde, 190

Utilisation de la source d'alimentation de secours, 383
VBScript, 16
Vérification de l'intégrité de l'application, 122
Vers de réseau, 18
Virus, 17
Virus traditionnels, 17
Viruses, 17
Virware, 17

ANNEXE D. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mé-

moire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous

quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du

non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus ;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats) ;

(c) Perte de moyens de paiement ;

(d) Perte d'économies prévues ;

(e) Perte de marché ;

(f) Perte d'occasions commerciales ;

(g) Perte de clientèle ;

(h) Atteinte à l'image ;

(i) Perte, endommagement ou corruption des données ; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

--- Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.