

# Kaspersky Security for Windows Server

Manuel de l'administrateur

*Version du produit : 10.1.2.996*

Chers utilisateurs !

Merci d'avoir choisi Kaspersky Lab en tant que fournisseur de logiciels de sécurité. Nous espérons que ce document vous aidera à utiliser nos produits.

Attention ! Ce document demeure la propriété de Kaspersky Lab AO (ci-après, Kaspersky Lab). Il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie et diffusion illicites de ce document, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément à la législation applicable.

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

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

Kaspersky Lab se réserve le droit de modifier ce document sans préavis.

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

Les marques déposées et les marques de service citées dans ce document appartiennent à leurs propriétaires respectifs.

Date de révision du document : 12/04/2019

© 2019 AO Kaspersky Lab. Tous droits réservés.

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

# Contents

A propos du guide.....	14
Dans ce document.....	14
Conventions.....	17
Sources d'informations sur Kaspersky Security for Windows Server.....	18
Sources de données pour des consultations indépendantes.....	18
Discussion sur les applications Kaspersky Lab dans la communauté.....	19
Kaspersky Security for Windows Server.....	20
A propos de Kaspersky Security for Windows Server.....	20
Nouveautés.....	23
Kit de distribution.....	23
Configurations logicielle et matérielle requises.....	25
Configuration requise pour le serveur sur lequel Kaspersky Security for Windows Server est installé.....	26
Configuration requise pour le périphérique de stockage NAS protégé.....	28
Configuration requise pour l'ordinateur sur lequel la Console de l'application est installée.....	29
Exigences fonctionnelles et restrictions.....	31
Installation et désinstallation.....	31
Protection du trafic.....	31
Moniteur d'intégrité des fichiers.....	32
Gestion du pare-feu.....	33
Autres restrictions.....	34
Installation et suppression de l'application.....	36
Codes des composants logiciel de Kaspersky Security for Windows Server pour le service Windows Installer.....	36
Composants logiciels de Kaspersky Security for Windows Server.....	37
Ensemble des "Outils d'administration" des composants logiciels.....	39
Modifications introduites dans le système après l'installation de Kaspersky Security for Windows Server.....	40
Processus de Kaspersky Security for Windows Server.....	43
Paramètres d'installation et de désinstallation et options de ligne de commande correspondantes pour le service Windows Installer.....	44
Journaux d'installation et de désinstallation de Kaspersky Security for Windows Server.....	47
Planification de l'installation.....	47
Sélection des outils d'administration.....	48
Sélection du type d'installation.....	49
Installation et suppression de l'application à l'aide de l'assistant.....	50
Installation à l'aide de l'Assistant d'installation.....	50
Modification de la sélection de composants et réparation de Kaspersky Security for Windows Server.....	62
Suppression à l'aide de l'Assistant d'installation.....	63
Installation et suppression de l'application via la ligne de commande.....	65
A propos de l'installation et de la désinstallation de Kaspersky Security for Windows Server via la ligne de commande.....	66

Exemple de commandes pour l'installation de Kaspersky Security for Windows Server .....	66
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	68
Ajout et suppression de composants. Exemples de commandes .....	69
Désinstallation de Kaspersky Security for Windows Server. Exemples de commandes .....	69
Codes de retour .....	70
Installation et suppression de l'application via Kaspersky Security Center .....	71
Informations générales sur l'installation via Kaspersky Security Center .....	72
Privilèges pour l'installation ou la désinstallation de Kaspersky Security for Windows Server .....	72
Installation de Kaspersky Security for Windows Server via Kaspersky Security Center .....	73
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	74
Installation de la console de l'application via Kaspersky Security Center .....	75
Désinstallation de Kaspersky Security for Windows Server via Kaspersky Security Center .....	76
Installation et suppression via les stratégies de groupe Active Directory .....	76
Installation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory ..	76
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	77
Désinstallation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory .....	78
Vérification des fonctions de Kaspersky Security for Windows Server. Utilisation du virus d'essai EICAR ....	78
A propos du virus d'essai EICAR .....	79
Vérification de la Protection en temps réel et de l'Analyse à la demande .....	80
Interface de l'application .....	82
Licence de l'application .....	83
A propos du Contrat de licence utilisateur final .....	83
A propos de la licence .....	84
A propos du certificat de licence .....	84
A propos de la clé .....	85
A propos du fichier clé .....	85
A propos du code d'activation .....	85
A propos de l'abonnement .....	86
A propos de la collecte des données .....	86
Activation de l'application à l'aide d'une clé de licence .....	89
Consultation des informations sur la licence active .....	89
Restriction des fonctions à l'expiration de la licence .....	92
Renouvellement de la licence .....	93
Suppression d'une clé .....	93
Utilisation du plug-in d'administration .....	95
Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center .....	95
Administration des paramètres de l'application .....	97
Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center .....	97
Navigation .....	98
Configuration des paramètres généraux de l'application dans Kaspersky Security Center .....	99

Configuration des paramètres de la quarantaine et de la Sauvegarde dans Kaspersky Security Center	105
Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués.....	106
A propos de la configuration des journaux et notifications .....	108
Création et configuration des stratégies .....	116
Création d'une stratégie.....	117
Sections contenant les paramètres de stratégie de Kaspersky Security for Windows Server .....	119
Configuration de stratégie .....	123
Création et configuration de tâches via Kaspersky Security Center .....	124
A propos de la création de tâches dans Kaspersky Security Center .....	124
Création d'une tâche dans Kaspersky Security Center .....	125
Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center.....	127
Configuration des tâches de groupe dans Kaspersky Security Center.....	128
Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center .....	136
Programmation des tâches.....	138
Génération de rapports dans Kaspersky Security Center .....	140
Utilisation de la console de Kaspersky Security for Windows Server .....	143
Paramètres de Kaspersky Security for Windows Server dans la Console de l'application.....	143
A propos de la console de Kaspersky Security for Windows Server .....	150
Interface de la console de Kaspersky Security for Windows Server .....	151
Icône de la barre d'état système dans la zone de notification.....	154
Administration de Kaspersky Security for Windows Server via la Console de l'application sur un autre ordinateur.....	156
Administration des tâches de Kaspersky Security for Windows Server .....	156
Catégories de tâche de Kaspersky Security for Windows Server .....	156
Lancement / suspension / rétablissement / arrêt manuel des tâches .....	157
Programmation des tâches.....	157
Utilisation des comptes utilisateur pour l'exécution des tâches .....	159
Importation et exportation des paramètres.....	161
Utilisation des modèles de paramètres de sécurité.....	164
Consultation de l'état de la protection et des informations de Kaspersky Security for Windows Server .....	167
Interface de diagnostic compacte .....	173
A propos de l'interface de diagnostic compacte .....	173
Révision de l'état de Kaspersky Security for Windows Server via l'interface de diagnostic compacte.....	174
Révision des statistiques des événements de sécurité.....	175
Révision de l'activité en cours de l'application .....	175
Configuration de l'écriture de fichiers dump et de fichiers de trace .....	176
Mise à jour des bases de données et des modules de l'application Kaspersky Security for Windows Server .....	178
A propos des tâches de mise à jour .....	178
A propos de la mise à jour des modules de l'application Kaspersky Security for Windows Server.....	179
A propos des mises à jour des bases de l'application Kaspersky Security for Windows Server .....	180



Schémas de mise à jour des bases et des modules des applications antivirus dans l'entreprise .....	180
Configuration des tâches de mise à jour .....	184
Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server .....	190
Remise à l'état antérieur à la mise à jour des modules de l'application .....	191
Statistiques sur les tâches de mise à jour .....	191
Isolement et copie de sauvegarde des objets .....	193
Isolement des objets probablement infectés. Quarantaine .....	193
Création de copies de sauvegarde des objets. Sauvegarde .....	203
Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués .....	209
Enregistrement des événements. Journaux de Kaspersky Security for Windows Server .....	213
Méthodes d'enregistrement des événements de Kaspersky Security for Windows Server .....	213
Journal d'audit système .....	214
Journaux d'exécution de la tâche .....	216
Journaux de sécurité .....	220
Consultation du journal des événements de Kaspersky Security for Windows Server dans l'observateur d'événements .....	220
Configuration des paramètres des journaux dans la console de Kaspersky Security for Windows Server .....	221
Configuration des notifications .....	227
Moyens de notification de l'administrateur et des utilisateurs .....	227
Configuration des notifications de l'administrateur et des utilisateurs .....	228
Lancement et arrêt de Kaspersky Security for Windows Server .....	231
Lancement et arrêt du plug-in d'administration de Kaspersky Security for Windows Server .....	231
Lancement de la console de Kaspersky Security for Windows Server depuis le menu Démarrer .....	231
Lancement et arrêt du service Kaspersky Security .....	232
Lancement des composants Kaspersky Security for Windows Server en mode sans échec du système d'exploitation .....	234
A propos de l'utilisation de Kaspersky Security for Windows Server en mode sans échec du système d'exploitation .....	234
Lancement de Kaspersky Security for Windows Server en mode sans échec .....	235
Auto-défense de Kaspersky Security for Windows Server .....	236
A propos de l'auto-défense de Kaspersky Security for Windows Server .....	236
Protection contre les modifications des dossiers avec les composants Kaspersky Security for Windows Server installés .....	236
Protection contre les modifications des clés de registre de Kaspersky Security for Windows Server .....	236
Enregistrement du service Kaspersky Security en tant que service protégé .....	237
Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server .....	239
A propos des autorisations d'administration de Kaspersky Security for Windows Server .....	239
A propos des autorisations d'administration des services enregistrés .....	241
A propos des autorisations d'administration du Service Kaspersky Security .....	241
A propos des autorisations d'accès au Service Kaspersky Security Management .....	243
Configuration des autorisations d'accès à l'administration de Kaspersky Security for Windows Server et au Service Kaspersky Security .....	244

Accès protégé par mot de passe aux fonctions de Kaspersky Security for Windows Server .....	246
Configuration des autorisations d'accès dans Kaspersky Security Center .....	246
Protection des fichiers en temps réel.....	248
A propos de la tâche Protection des fichiers en temps réel .....	248
A propos de la zone de protection de la tâche et des paramètres de sécurité .....	249
A propos de la zone de protection virtuelle .....	250
Zones de protection prédéfinies .....	250
Niveaux de sécurité prédéfinis .....	251
Extensions de fichiers analysés par défaut dans la tâche Protection des fichiers en temps réel .....	253
Paramètres par défaut de la tâche Protection des fichiers en temps réel.....	256
Administration de la tâche de protection des fichiers en temps réel via le plug-in d'administration .....	257
Navigation.....	257
Configuration de la tâche Protection des fichiers en temps réel .....	258
Création et configuration de la zone de protection de la tâche .....	263
Configuration manuelle des paramètres de sécurité.....	264
Administration de la tâche de protection des fichiers en temps réel via la Console de l'application .....	271
Navigation.....	271
Accès aux paramètres de la zone de protection des fichiers en temps réel.....	271
Accès aux paramètres de la tâche Protection des fichiers en temps réel .....	272
Configuration de la tâche Protection des fichiers en temps réel .....	272
Constitution de la zone de protection .....	276
Configuration manuelle des paramètres de sécurité.....	279
Statistiques de la tâche Protection des fichiers en temps réel.....	286
Monitoring des scripts.....	289
A propos de la tâche Monitoring des scripts.....	289
Paramètres par défaut de la tâche Monitoring des scripts .....	290
Configuration des paramètres de la tâche Monitoring des scripts via le Plug-in d'administration .....	290
Configuration des paramètres de la tâche Monitoring des scripts via la Console de l'application.....	292
Statistiques de la tâche Monitoring des scripts .....	293
Utilisation du KSN.....	295
A propos de la tâche Utilisation du KSN.....	295
Paramètres de la tâche Utilisation du KSN par défaut .....	297
Administration de l'utilisation du KSN via le plug-in d'administration .....	297
Configuration de la tâche Utilisation du KSN via le plug-in d'administration.....	298
Configuration du traitement des données via le plug-in d'administration.....	300
Administration de l'utilisation du KSN via la Console de l'application .....	302
Configuration de la tâche Utilisation du KSN via la Console de l'application.....	302
Configuration du traitement des données via la Console de l'application.....	304
Configuration du transfert de données supplémentaires.....	306
Statistiques de la tâche Utilisation du KSN .....	307

Protection du trafic .....	309
A propos de la tâche Protection du trafic.....	309
A propos des règles de protection du trafic .....	310
Protection contre les menaces email.....	311
Liste des catégories.....	312
Paramètres de niveau de protection prédéfini.....	316
Paramètres par défaut de la tâche Protection du trafic .....	317
Administration de la Protection du trafic via le plug-in d'administration .....	318
Navigation.....	318
Configuration de la tâche Protection du trafic .....	319
Configuration de la protection contre les applications malveillantes sur Internet .....	324
Configuration de la protection contre les menaces email .....	327
Configuration du traitement des adresses et des sites Internet .....	327
Configuration du Contrôle Internet .....	329
Administration de la protection du trafic via la Console de l'application.....	333
Navigation.....	333
Configuration de la tâche Protection du trafic .....	334
Configuration de la protection contre les applications malveillantes sur Internet .....	338
Configuration de la protection contre les menaces email .....	341
Configuration du traitement des adresses et des sites Internet .....	342
Configuration du Contrôle Internet .....	343
Protection contre le chiffrement.....	348
A propos de la tâche Protection contre le chiffrement.....	348
Statistiques de la tâche Protection contre le chiffrement .....	349
Paramètres de la tâche Protection contre le chiffrement par défaut .....	349
Configuration des paramètres de la tâche Protection contre le chiffrement via le Plug-in d'administration ..	350
Paramètres des tâches de groupe .....	351
Constitution de la zone de protection .....	352
Ajout d'exclusions .....	353
Configuration des paramètres de la tâche Protection contre le chiffrement via la Console de l'application ..	355
Constitution de la zone de protection .....	355
Paramètres des tâches de groupe .....	357
Ajout d'exclusions .....	357
Contrôle du lancement des applications.....	359
A propos de la tâche Contrôle du lancement des applications .....	359
A propos des règles du contrôle du lancement des applications .....	360
A propos du contrôle de la distribution des logiciels .....	362
A propos l'utilisation du KSN dans la tâche Contrôle du lancement des applications .....	365
Création des règles du Contrôle du lancement des applications .....	366
Paramètres de la tâche Contrôle du lancement des applications par défaut.....	368
Administration du Contrôle du lancement des applications via le plug-in d'administration .....	371



Navigation.....	371
Configuration des paramètres de la tâche Contrôle du lancement des applications .....	373
Configuration du contrôle de la distribution des logiciels .....	376
Configuration de la tâche Génération des règles du Contrôle du lancement des applications .....	379
Configuration des règles du Contrôle du lancement des applications via Kaspersky Security Center.....	381
Création d'une tâche Génération des règles du Contrôle du lancement des applications .....	390
Utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center .....	395
Administration du Contrôle du lancement des applications via la Console de l'application .....	396
Navigation.....	396
Configuration des paramètres de la tâche Contrôle du lancement des applications .....	397
Configuration des règles du Contrôle du lancement des applications .....	404
Configuration d'une tâche Génération des règles du Contrôle du lancement des applications.....	410
Contrôle des périphériques.....	415
A propos de la tâche Contrôle des périphériques .....	415
A propos des règles du Contrôle des périphériques .....	416
A propos de la formation de la liste des règles du Contrôle des périphériques .....	418
A propos de la tâche Génération des règles du Contrôle des périphériques.....	420
Scénarios de création de règles du Contrôle des périphériques.....	420
Paramètres par défaut de la tâche Contrôle des périphériques.....	421
Administration du Contrôle des périphériques via le plug-in d'administration .....	422
Navigation.....	422
Configuration de la tâche Contrôle des périphériques .....	424
Génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center.....	425
Configuration de la tâche Génération des règles du Contrôle des périphériques .....	427
Configuration de la tâche Contrôle des périphériques via Kaspersky Security Center.....	428
Administration du Contrôle des périphériques via la Console de l'application .....	433
Navigation.....	434
Configuration des paramètres de la tâche Contrôle des périphériques .....	435
Configuration des règles du Contrôle des périphériques .....	436
Configuration de la tâche Génération des règles du Contrôle des périphériques .....	440
Gestion du pare-feu .....	443
A propos de la tâche Gestion du pare-feu.....	443
A propos des règles du pare-feu .....	444
Paramètres par défaut de la tâche Gestion du pare-feu .....	446
Administration des règles du pare-feu via le plug-in d'administration .....	446
Activation et désactivation des règles du pare-feu.....	446
Ajout manuel de règles du pare-feu .....	447
Suppression de règles du pare-feu .....	449
Administration des règles du pare-feu via la Console de l'application .....	450
Activation et désactivation des règles du pare-feu.....	450

Ajout manuel de règles du pare-feu .....	451
Suppression de règles du pare-feu .....	452
Moniteur d'intégrité des fichiers .....	453
A propos de la tâche Moniteur d'intégrité des fichiers .....	453
A propos des règles de monitoring des opérations sur les fichiers .....	454
Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers .....	457
Administration du Moniteur d'intégrité des fichiers via le plug-in d'administration .....	458
Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers .....	458
Configuration des règles de monitoring .....	459
Administration du Moniteur d'intégrité des fichiers via la Console de l'application .....	462
Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers .....	463
Configuration des règles de monitoring .....	463
Inspection des journaux .....	467
A propos de la tâche Inspection des journaux .....	467
Paramètres de la tâche Inspection des journaux par défaut .....	468
Administration des règles d'inspection des journaux via le plug-in d'administration .....	469
Administration des règles de tâches prédéfinies via le plug-in d'administration .....	469
Ajout de règles d'inspection des journaux via le plug-in d'administration .....	471
Administration des règles d'inspection des journaux via la Console de l'application .....	472
Administration des règles de tâches prédéfinies via la Console de l'application .....	473
Configuration des règles d'inspection des journaux .....	474
Analyse à la demande .....	476
A propos des tâches d'analyse à la demande .....	476
A propos de la zone d'analyse .....	477
Zones d'analyse prédéfinies .....	477
Analyse des fichiers de stockage dans le cloud .....	479
Paramètres de sécurité du nœud sélectionné dans les tâches d'analyse à la demande .....	480
A propos des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	481
A propos de l'analyse des disques amovibles .....	483
Paramètres par défaut de la tâche d'analyse à la demande .....	484
Administration des tâches d'analyse à la demande via le plug-in d'administration .....	486
Navigation .....	486
Création d'une tâche d'analyse à la demande .....	488
Configuration de la zone d'analyse de la tâche .....	493
Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	494
Configuration manuelle des paramètres de sécurité .....	495
Configuration de l'analyse des disques amovibles .....	502
Administration des tâches d'analyse à la demande via Console de l'application .....	502
Navigation .....	503
Création et configuration d'une tâche d'analyse à la demande .....	503
Zone d'analyse dans les tâches d'analyse à la demande .....	506

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	510
Configuration manuelle des paramètres de sécurité .....	510
Analyse des disques amovibles .....	517
Statistiques des tâches d'analyse à la demande .....	518
Zone de confiance .....	520
A propos de la zone de confiance .....	520
Administration de la Zone de confiance via le plug-in d'administration .....	522
Navigation .....	522
Configuration des paramètres de la Zone de confiance via le plug-in d'administration .....	523
Administration de la Zone de confiance via la Console de l'application .....	528
Application de la Zone de confiance aux tâches dans la Console de l'application .....	528
Configuration des paramètres de la Zone de confiance dans la Console de l'application .....	529
Protection contre les exploits .....	535
A propos de la Protection contre les exploits .....	535
Administration de la Protection contre les exploits via le plug-in d'administration .....	536
Navigation .....	537
Configuration des paramètres de protection de la mémoire des processus .....	538
Ajout d'un processus protégé .....	539
Administration de la Protection contre les exploits via la Console de l'application .....	540
Navigation .....	540
Configuration des paramètres de protection de la mémoire des processus .....	541
Ajout d'un processus protégé .....	542
Techniques de protection contre les exploits .....	544
Administration du stockage hiérarchique .....	545
A propos du stockage hiérarchique .....	545
Configuration des paramètres du système HSM via le plug-in d'administration .....	546
Configuration des paramètres du système HSM via la Console de l'application .....	547
Intégration aux systèmes tiers .....	549
Contrôle des performances. Compteurs de Kaspersky Security for Windows Server .....	549
Compteurs de performance pour l'application Moniteur système .....	549
Compteurs et interruptions SNMP de Kaspersky Security for Windows Server .....	556
Intégration à WMI .....	565
Utilisation de Kaspersky Security for Windows Server depuis la ligne de commande .....	569
Commandes de la ligne de commande .....	569
Affichage de l'aide sur les commandes de Kaspersky Security for Windows Server. KAVSHELL HELP .....	572
Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP .....	572
Analyse de la zone indiquée. KAVSHELL SCAN .....	573
Lancement de la tâche Analyse des zones critiques. KAVSHELL SCANCritical .....	577
Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK .....	578
Enregistrement de KAVFS en tant que processus protégé par le système. KAVSHELL CONFIG .....	579
Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP .....	580

Administration de la tâche Contrôle du lancement des applications KAVSHELL APPCONTROL /CONFIG.....	581
Génération des règles du contrôle du lancement des applications KAVSHELL APPCONTROL /GENERATE.....	582
Enrichissement de la liste des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL.....	584
Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier. KAVSHELL DEVCONTROL.....	585
Lancement de la tâche de mise à jour des bases de l'application de Kaspersky Security for Windows Server. KAVSHELL UPDATE.....	586
Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server. KAVSHELL ROLLBACK.....	589
Gestion de l'inspection des journaux. KAVSHELL TASK LOG-INSPECTOR.....	590
Activation de l'application KAVSHELL LICENSE.....	590
Activation, configuration et désactivation d'un journal de traçage. KAVSHELL TRACE.....	591
Défragmentation des fichiers journaux de Kaspersky Security for Windows Server. KAVSHELL VACUUM.....	594
Purge de la base iSwift. KAVSHELL FBRESET.....	595
Activation et désactivation de la création de fichiers dump. KAVSHELL DUMP.....	595
Importation des paramètres. KAVSHELL IMPORT.....	596
Exportation des paramètres. KAVSHELL EXPORT.....	597
Intégration avec Microsoft Operation Management Suite. KAVSHELL OMSINFO.....	597
Codes de retour de la ligne de commande.....	598
Codes de retour des instructions KAVSHELL START et KAVSHELL STOP.....	599
Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCritical.....	599
Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR.....	600
Codes de retour de l'instruction KAVSHELL TASK.....	600
Codes de retour de l'instruction KAVSHELL RTP.....	601
Codes de retour de l'instruction KAVSHELL UPDATE.....	601
Codes de retour de l'instruction KAVSHELL ROLLBACK.....	602
Codes de retour de l'instruction KAVSHELL LICENSE.....	602
Codes de retour de l'instruction KAVSHELL TRACE.....	603
Codes de retour de l'instruction KAVSHELL FBRESET.....	603
Codes de retour de l'instruction KAVSHELL DUMP.....	603
Codes de retour de l'instruction KAVSHELL IMPORT.....	604
Codes de retour de l'instruction KAVSHELL EXPORT.....	604
Contacteur le Support Technique.....	606
Modes d'obtention de l'assistance technique.....	606
Assistance technique via téléphone.....	606
Assistance technique via Kaspersky CompanyAccount.....	607
Utilisation du fichier de trace et du script AVZ.....	607

Glossaire .....	609
Kaspersky Lab .....	614
Information sur le code tiers .....	615
Avis de marques déposées .....	616
Index .....	617

# A propos du guide

Le Manuel de l'administrateur de Kaspersky Security for Windows Server 10.1 (ci-après "Kaspersky Security for Windows Server") s'adresse aux spécialistes qui installent et administrent Kaspersky Security for Windows Server sur tous les périphériques protégés ainsi qu'aux spécialistes chargés de l'assistance technique des organisations qui utilisent Kaspersky Security for Windows Server.

Ce manuel contient des informations sur la configuration et l'utilisation de Kaspersky Security for Windows Server.

Il renseigne également les sources d'informations sur l'application et explique la marche à suivre pour bénéficier du Support Technique.

## Contenu du chapitre

Dans ce document.....	<a href="#">14</a>
Conventions.....	<a href="#">17</a>

## Dans ce document

Le Manuel de l'administrateur de Kaspersky Security for Windows Server contient les sections suivantes :

### Sources d'informations sur Kaspersky Security for Windows Server

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

Vous pouvez choisir celle qui vous convient le mieux en fonction du niveau d'importance et de l'urgence de la question.

### Kaspersky Security for Windows Server

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Security for Windows Server. Elle reprend la configuration matérielle et logicielle requise pour l'application.

### Installation et suppression de l'application

Cette section explique pas à pas la procédure d'installation et de désinstallation de Kaspersky Security for Windows Server.

### Interface de l'application

Cette section contient des informations sur les éléments de l'interface de Kaspersky Security for Windows Server.

### Licence de l'application

Cette section présente les principales notions relatives à la licence de l'application.

### Utilisation du plug-in d'administration

Cette section fournit des informations sur le plug-in d'administration de Kaspersky Security for Windows Server et décrit la procédure d'administration de l'application installée sur un serveur protégé ou sur un groupe de serveurs.



## Utilisation de la Console de l'application

Cette section fournit des informations sur la console de Kaspersky Security for Windows Server et sur l'administration de l'application via la console de l'application installée sur le serveur protégé ou sur un autre ordinateur.

## Lancement et arrêt de Kaspersky Security for Windows Server

Cette section fournit des informations sur le lancement de la console de l'application, ainsi que sur le lancement et l'arrêt du service Kaspersky Security.

## Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Security for Windows Server et des services Windows® enregistrés par l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

## Protection des fichiers en temps réel

Cette section contient des informations sur la tâche Protection des fichiers en temps réel et les instructions sur la configuration de cette tâche.

## Monitoring des scripts

Cette section contient des informations sur la tâche Monitoring des scripts et les instructions sur la configuration de cette tâche.

## Utilisation du KSN

Cette section contient des informations sur la tâche Utilisation du KSN et les instructions sur la configuration de cette tâche.

## Protection du trafic

Cette section contient des informations sur la tâche Protection du trafic et les instructions sur la configuration de cette tâche.

## Protection contre le chiffrement

Cette section contient des informations sur la tâche Protection contre le chiffrement et sur sa configuration.

## Contrôle du lancement des applications

Cette section contient des informations sur la tâche de Contrôle du lancement des applications et les instructions sur la configuration de cette tâche.

## Contrôle des périphériques

Cette section contient les informations sur la tâche Contrôle des périphériques et les instructions de configuration de ses paramètres.

## Gestion du pare-feu

Cette section contient des informations sur la tâche Gestion du pare-feu et sa configuration.

## Moniteur d'intégrité des fichiers

Cette section contient des informations sur le lancement et la configuration de la tâche Moniteur d'intégrité des fichiers.

## [Inspection des journaux](#)

Cette section contient des informations sur la tâche Inspection des journaux et la configuration de ses paramètres.

## [Analyse à la demande](#)

Cette section contient des informations sur les tâches d'analyse à la demande et explique la configuration des paramètres de ces tâches ainsi que la configuration des paramètres de la sécurité du serveur protégé.

## [Zone de confiance](#)

Cette section contient des informations sur la zone de confiance de Kaspersky Security for Windows Server, ainsi que des instructions pour ajouter des objets à la zone de confiance lors de l'exécution des tâches.

## [Protection contre les exploits](#)

Cette section contient les instructions de configuration des paramètres de la protection de la mémoire des processus contre l'exploitation des vulnérabilités.

## [Administration du stockage hiérarchique](#)

Cette section contient des informations sur l'analyse antivirus des fichiers qui se trouvent dans des stockages hiérarchiques et dans des systèmes de sauvegarde.

## [Intégration aux systèmes tiers](#)

Cette section décrit l'intégration de Kaspersky Security for Windows Server aux fonctions et technologies tierces.

## [Utilisation de Kaspersky Security for Windows Server depuis la ligne de commande](#)

Cette section décrit l'utilisation de Kaspersky Security for Windows Server via la ligne de commande.

## [Contacter le Support Technique](#)

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

## [Glossaire](#)

Cette section reprend les termes utilisés dans ce document et leur définition.

## [Kaspersky Lab](#)

Cette section contient des informations sur Kaspersky Lab.

## [Information sur le code tiers](#)

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

## [Avis de marques déposées](#)

Cette section reprend les marques de commerce citées dans le document et leurs détenteurs respectifs.

## [Index](#)

Cette section permet de trouver rapidement les informations que vous cherchez dans le document.

# Conventions

Ce document utilise des conventions de style (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui pourraient avoir des conséquences fâcheuses.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires et des conseils.
Exemple : ...	Les exemples sont présentés sur un fond bleu sous le titre "Exemple".
La <i>mise à jour</i> , c'est ... L'événement <i>Bases dépassées</i> survient.	Les éléments suivants sont en <i>italique</i> dans le texte : <ul style="list-style-type: none"> <li>• nouveaux termes ;</li> <li>• noms des états et des événements de l'application.</li> </ul>
Appuyez sur la touche <b>ENTER</b> . Appuyez sur la combinaison de touches <b>ALT+F4</b> .	Les noms des touches du clavier sont en caractères <b>gras</b> et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton <b>Activer</b> .	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères <b>gras</b> .
► <i>Pour programmer une tâche, procédez comme suit :</i>	Les phrases d'introduction des instructions sont en italique et sont accompagnées d'une flèche.
Dans la ligne de commande, saisissez le texte <code>help</code> Les informations suivantes s'affichent : Indiquez la date au format JJ:MM:AA.	Les types de texte suivants apparaissent dans un style spécial : <ul style="list-style-type: none"> <li>• Texte de la ligne de commande ;</li> <li>• Texte des messages affichés sur l'écran par l'application ;</li> <li>• Données à saisir via le clavier.</li> </ul>
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace le nom de la variable. Par ailleurs, les chevrons sont omis.

# Sources d'informations sur Kaspersky Security for Windows Server

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

Vous pouvez choisir celle qui vous convient le mieux en fonction du niveau d'importance et de l'urgence de la question.

## Contenu du chapitre

Sources de données pour des consultations indépendantes .....	<a href="#">18</a>
Discussion sur les applications Kaspersky Lab dans la communauté .....	<a href="#">19</a>

## Sources de données pour des consultations indépendantes

Vous pouvez utiliser les sources suivantes pour rechercher vous-même des informations sur Kaspersky Security for Windows Server :

- Page de Kaspersky Security for Windows Server sur le site Internet de Kaspersky Lab.
- Page de Kaspersky Security for Windows Server sur le site du Support Technique (Base de connaissances).
- Manuels.

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky Lab : <https://support.kaspersky.com/fr>.

L'utilisation des sources d'informations sur le site Internet de Kaspersky Lab requiert une connexion à Internet.

### Page de Kaspersky Security for Windows Server sur le site Internet de Kaspersky Lab

La page de Kaspersky Security for Windows Server

<https://www.kaspersky.fr/small-to-medium-business-security/windows-server-security> fournit des informations générales sur l'application, sur ses fonctionnalités et ses particularités.

La page de Kaspersky Security for Windows Server affiche un lien vers le magasin en ligne. Dans la boutique, vous pourrez acheter l'application ou prolonger vos droits d'utilisation.

### Page de Kaspersky Security for Windows Server dans la base des connaissances

La base des connaissances est une section du site du Support Technique.

La page de Kaspersky Security for Windows Server dans la Base des connaissances

<https://support.kaspersky.com/fr/ksws10> permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la Base de connaissances peuvent répondre à des questions qui concernent non seulement Kaspersky Security for Windows Server mais également d'autres applications de Kaspersky Lab. Ces articles peuvent également contenir des actualités du Support technique.

#### Documentation de Kaspersky Security for Windows Server

Le Manuel de l'administrateur de Kaspersky Security for Windows Server reprend les informations relatives à l'installation, à la désinstallation, à la configuration des paramètres et à l'utilisation de l'application.

## Discussion sur les applications Kaspersky Lab dans la communauté

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs dans notre communauté <https://community.kaspersky.com/>.

Sur cette communauté, vous pouvez consulter les sujets publiés, ajouter des commentaires, et créer de nouveaux sujets de discussion.

# Kaspersky Security for Windows Server

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Security for Windows Server. Elle reprend la configuration matérielle et logicielle requise pour l'application.

## Contenu du chapitre

A propos de Kaspersky Security for Windows Server .....	<a href="#">20</a>
Nouveautés .....	<a href="#">23</a>
Kit de distribution .....	<a href="#">23</a>
Configurations logicielle et matérielle requises .....	<a href="#">25</a>
Exigences fonctionnelles et restrictions .....	<a href="#">31</a>

## A propos de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server protège les serveurs tournant sous les systèmes d'exploitation Microsoft® Windows et les périphériques de stockage NAS contre les virus et autres menaces informatiques qui se propagent sur les serveurs et les périphériques de stockage NAS via l'échange de fichiers. Kaspersky Security for Windows Server a été développé pour les intranets des grandes et des moyennes entreprises. Les utilisateurs de Kaspersky Security for Windows Server sont les administrateurs de réseau de l'organisation et les personnes chargées de la protection antivirus de ce réseau.

Vous pouvez installer Kaspersky Security for Windows Server sur les serveurs avec les rôles suivants :

- Services de certificat Active Directory®
- Services de domaine Active Directory
- Services de fédération Active Directory
- Services Active Directory Lightweight Directory
- Services de gestion des droits Active Directory
- Device Health Attestation
- Serveur DHCP
- Serveur DNS
- Serveur de fax
- Services de fichier et de stockage
- Services Host Guardian
- Hyper-V®
- Contrôleur réseau



- Services de stratégie réseau et d'accès
- Services d'impression et de document
- Accès à distance
- Services de bureau Remote Desktop Services
- Services d'activation de volume
- Serveur Internet (IIS)
- Services de déploiement Windows
- Services de mise à jour Windows Server®

Kaspersky Security for Windows Server peut être géré de la manière suivante :

- via la console de l'application installée sur le même serveur que Kaspersky Security for Windows Server ou sur un autre ordinateur ;
- via la ligne de commande ;
- via la Console d'administration de Kaspersky Security Center.

Vous pouvez utiliser également l'application Kaspersky Security Center pour l'administration centralisée de la protection de nombreux serveurs doté chacun de Kaspersky Security for Windows Server.

Il est possible de consulter les compteurs de performance de Kaspersky Security for Windows Server pour l'application « Moniteur système » ainsi que les compteurs et les interruptions SNMP.

### Composants et fonctions de Kaspersky Security for Windows Server

L'application intègre les modules suivants :

- **Protection des fichiers en temps réel.** Kaspersky Security for Windows Server analyse les objets à l'accès. Kaspersky Security for Windows Server analyse les objets suivants :
  - Les fichiers ;
  - Flux alternatifs des systèmes de fichiers (flux NTFS) ;
  - L'enregistrement de démarrage principal et les secteurs d'amorçage des disques durs locaux ou amovibles ;
  - Fichiers conteneurs Windows Server 2016 et Windows Server 2019.
- **Analyse à la demande.** Kaspersky Security for Windows Server recherche une fois des virus et autres menaces informatique dans la zone indiquée. L'application analyse les fichiers, la mémoire et les objets de démarrage sur un serveur protégé.
- **Protection RPC des stockages réseau connectés et Protection ICAP des stockages réseau connectés.** Kaspersky Security for Windows Server installé sur un serveur tournant sous un système d'exploitation Microsoft Windows protège les périphériques de stockage NAS contre les virus et autres menaces informatiques qui s'introduisent sur les serveurs via l'échange de fichiers.
- **Contrôle du lancement des applications.** Ce composant surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus.
- **Contrôle des périphériques.** Ce composant contrôle l'enregistrement et l'utilisation des périphériques de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger l'ordinateur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou des périphériques externes d'un autre type connectés par USB.

- **Protection contre le chiffrement et Protection contre le chiffrement pour NetApp.** Les composants protègent les dossiers partagés sur les serveurs et les périphériques de stockage NAS contre le chiffrement malveillant en bloquant les hôtes qui affichent une activité malveillante.
- **Monitoring des scripts.** Ce composant contrôle l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies.
- **Protection du trafic.** Ce module intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informations connues ou autres sur le serveur protégé.
- **Gestion du pare-feu.** Ce composant permet d'administrer le pare-feu Windows : il permet de configurer les paramètres et les règles du pare-feu du système d'exploitation et interdit toute possibilité de configuration du pare-feu externe.
- **Moniteur d'intégrité des fichiers.** Kaspersky Security for Windows Server détecte les modifications introduites dans les fichiers qui appartiennent aux zones de monitoring définies dans les paramètres de la tâche. Ces modifications peuvent signaler une violation de la sécurité sur le serveur protégé.
- **Inspection des journaux.** Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.

L'application peut remplir les fonctions suivantes :

- **Mise à jour des bases de l'application et Mise à jour des modules de l'application.** Kaspersky Security for Windows Server télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky Lab, depuis le Serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.
- **Quarantaine.** Kaspersky Security for Windows Server place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers le dossier *Quarantaine*. Pour des raisons de sécurité, une fois dans le dossier Quarantaine, les objets sont chiffrés.
- **Sauvegarde.** Kaspersky Security for Windows Server enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Probablement infecté* dans la *Sauvegarde* avant de procéder à la désinfection ou à la suppression de ces objets.
- **Notifications de l'administrateur et des utilisateurs.** Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Security for Windows Server et à l'état de la protection antivirus du serveur.
- **Importation et exportation des paramètres.** Vous pouvez exporter les paramètres de Kaspersky Security for Windows Server dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security for Windows Server depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.
- **Application des modèles.** Vous pouvez configurer manuellement les paramètres de sécurité du nœud dans l'arborescence des ressources fichier de l'ordinateur et enregistrer les valeurs définies comme un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Security for Windows Server.
- **Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server.** Vous pouvez configurer les autorisations d'administration de Kaspersky Security for Windows Server et des services Windows que l'application enregistre pour des utilisateurs ou des groupes d'utilisateurs.
- **Enregistrement des événements de l'application dans le journal.** Kaspersky Security for Windows Server enregistre les informations relatives aux paramètres de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution des tâches, aux événements associés avec Kaspersky Security for Windows Server et aux informations requises pour diagnostiquer les erreurs dans Kaspersky Security for

Windows Server.

- **Stockage hiérarchique.** Kaspersky Security for Windows Server peut fonctionner en mode de gestion de stockage hiérarchique (système HSM). Le recours aux systèmes HSM permet de transférer des données entre des disques locaux rapides et des périphériques lents de stockage d'informations de longue durée.
- **Zone de confiance.** Vous pouvez composer la liste des exclusions de la zone de protection ou d'analyse que Kaspersky Security for Windows Server appliquera aux tâches d'analyse à la demande et de protection en temps réel.
- **Protection contre les exploits.** Vous pouvez protéger la mémoire des processus contre l'exploitation des vulnérabilités à l'aide de l'Agent de protection intégré dans ce processus.
- **Stockage des ordinateurs bloqués.** Vous pouvez bloquer les ordinateurs distants qui tentent d'accéder aux dossiers réseau partagés du serveur si ces ordinateurs affichent une activité malveillante.

## Nouveautés

Kaspersky Security for Windows Server contient les nouveautés et les améliorations suivantes :

- Prise en charge des nouvelles versions des systèmes d'exploitation Microsoft Windows.
  - Windows Storage Server 2019 (x64)
  - Windows Server 2019 (x64)
- Le code d'activation ne peut pas s'afficher entièrement dans l'interface graphique de l'application.  
Le code d'activation déjà ajouté est partiellement masqué lors de son affichage dans l'interface graphique de l'application et ne peut être consulté entièrement par l'utilisateur.
- Moins de faux positifs dans la tâche Protection contre le chiffrement.  
Exclusions par défaut supplémentaires pour plusieurs types de fichiers afin d'éviter des faux positifs précis.

## Kit de distribution

Le kit de distribution contient une page de bienvenue au départ de laquelle vous pouvez réaliser les opérations suivantes :

- lancer l'assistant Installation de Kaspersky Security for Windows Server ;
- lancer l'assistant Installation de la console de Kaspersky Security for Windows Server ;
- lancer l'assistant d'installation du plug-in d'administration de Kaspersky Security for Windows Server pour gérer l'application via Kaspersky Security Center ;
- Lancez l'Assistant d'installation du Plug-in Kaspersky Security for Windows Server 10.1 pour Microsoft Outlook® (ci-après dénommé Microsoft Outlook) ;
- Lire le Manuel de l'administrateur ;
- Lisez le Manuel d'implantation pour la Protection des stockages réseau ;

- Ouvrez la page de Kaspersky Security for Windows Server <https://www.kaspersky.fr/small-to-medium-business-security/windows-server-security> sur le site Web de Kaspersky Lab ;
- Visitez le site Internet du Support technique <https://support.kaspersky.com/fr> ;
- lisez les informations relatives à la version actuelle de Kaspersky Security for Windows Server.

Le dossier \client contient les fichiers d'installation de la Console de l'application (ensemble de composants "Outils d'administration de Kaspersky Security for Windows Server") et un fichier avec le texte du Contrat de licence utilisateur final.

Le dossier \server contient :

- les fichiers d'installation des composants de Kaspersky Security for Windows Server sur un ordinateur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows ;
- le fichier d'installation du plug-in d'administration de Kaspersky Security for Windows Server via Kaspersky Security Center ;
- l'archive contenant les bases antivirus d'actualité au moment de l'édition de l'application ;
- un fichier contenant le texte du Contrat de licence utilisateur final et de la Politique de confidentialité.

Le dossier \setup contient les fichiers indispensables au lancement de l'application de bienvenue.

Le dossier \email\_plugin contient le paquet d'installation du Plug-in Microsoft Outlook et un fichier avec le texte du Contrat de licence utilisateur final.

Les fichiers du kit de distribution s'installent dans différents dossiers en fonction de leur rôle (cf. tableau ci-après).

Tableau 2. Fichiers u kit de distribution de Kaspersky Security for Windows Server

Fichier	Fonction
autorun.inf	Fichier de démarrage automatique de l'Assistant d'installation de Kaspersky Security for Windows Server pour l'installation de l'application depuis un support amovible.
ks4ws_admin_guide_fr.pdf	Manuel de l'administrateur.
ks4ws_netstorage_guide_fr.pdf	Manuel d'implantation pour la protection des stockages réseau.
migration.txt	Le fichier décrit la migration depuis les versions antérieures de l'application.
release_notes.txt	Ce fichier contient les informations relatives à la version.
setup.exe	Fichier d'accueil de lancement de l'application (lance setup.hta).
\client\ks4wstools_x86(x64).msi	Paquet d'installation du service Windows Installer ; installe la console de l'application sur le serveur protégé.
\client\license.txt	Texte du Contrat de licence utilisateur final
\client\setup.exe	Fichier de lancement de l'Assistant d'installation de l'ensemble des composants "Outils d'administration" (contient la console de l'application) ; lance le fichier du paquet d'installation ks4wstools.msi selon les paramètres d'installation définis dans l'Assistant.
\server\bases.cab	Archive contenant les bases antivirus d'actualité au moment de l'édition de l'application.

Fichier	Fonction
\\server\setup.exe	Fichier de lancement de l'assistant d'installation de Kaspersky Security for Windows Server sur le serveur protégé ; lance le fichier du paquet d'installation ks4ws.msi selon les paramètres d'installation définis dans l'assistant.
\\server\ks4ws_x86(x64).msi	Paquet d'installation du service Windows Installer ; installe Kaspersky Security for Windows Server sur le serveur protégé.
\\server\ks4ws.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de Kaspersky Security for Windows Server via Kaspersky Security Center.
\\server\klcfginst.exe	Programme d'installation du plug-in d'administration de Kaspersky Security for Windows Server via Kaspersky Security Center. Installez le plug-in d'administration sur chacun des serveurs dotés de la Console d'administration Kaspersky Security Center si vous avez l'intention de l'utiliser pour administrer Kaspersky Security for Windows Server.
\\server\license.txt	Texte du Contrat de licence utilisateur final et de la Politique de confidentialité.
\\setup\setup.hta	Fichier pour le lancement de l'application d'accueil.
\\email_plugin\ksmail_x86(x64).msi	Paquet d'installation de Windows Installer ; installe le Plug-in Microsoft Outlook sur le serveur protégé.
\\email_plugin\license.txt	Texte du Contrat de licence utilisateur final

Vous pouvez lancer les fichiers du kit de distribution depuis le cd. Si vous avez d'abord copié les fichiers sur le disque local, assurez-vous que la structure des fichiers du kit de distribution a été préservée.

## Configurations logicielle et matérielle requises

Cette section décrit toutes les configurations logicielle et matérielle requises pour le serveur protégé et les périphériques de stockage NAS.

### Dans cette section

Configuration requise pour le serveur sur lequel Kaspersky Security for Windows Server est installé .....	<a href="#">26</a>
Configuration requise pour le périphérique de stockage NAS protégé .....	<a href="#">28</a>
Configuration requise pour l'ordinateur sur lequel la Console de l'application est installée .....	<a href="#">29</a>

## Configuration requise pour le serveur sur lequel Kaspersky Security for Windows Server est installé

Avant d'installer Kaspersky Security for Windows Server, il convient de supprimer du serveur tout autre logiciel antivirus qui serait installé.

Avant d'installer Kaspersky Security for Windows Server 10.1, vous devez désinstaller Kaspersky Anti-Virus 8.0 for Windows Server Enterprise Edition. Vous pouvez installer Kaspersky Security for Windows Server 10.1 sans désinstaller Kaspersky Security 10 for Windows Server ou suivant.

### Configuration matérielle requise pour le serveur

Recommandations d'ordre général :

- systèmes compatibles x8664 avec un ou plusieurs processeurs ;
- Espace disque requis :
  - pour l'installation de tous les modules de l'application : 100 Mo
  - pour le téléchargement et le stockage des bases antivirus de l'application : 2 Go (recommandé)
  - pour l'enregistrement des objets en quarantaine et dans la sauvegarde : 400 Mo (recommandé)
  - pour l'enregistrement des journaux : 1 Go (recommandé)

Configuration minimale :

- Processeur : monocœur 1,4 GHz
- RAM : 1 Go
- Sous-système de disque : 4 Go d'espace libre

Configuration recommandée :

- Processeur : quadricœur 2,4 GHz
- RAM : 2 Go
- Sous-système de disque : 4 Go d'espace libre

### Configuration logicielle requise pour le serveur

Vous pouvez installer Kaspersky Security for Windows Server sur un serveur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows.

L'installation et l'utilisation de Kaspersky Security for Windows Server requièrent Microsoft Windows Installer 3.1 sur le serveur.

Vous pouvez installer Kaspersky Security for Windows Server sur un serveur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;



- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Server 2008 Core / Standard / Enterprise / Datacenter SP1 ou suivant ;

Vous pouvez installer Kaspersky Security for Windows Server sur un serveur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Server 2008 Standard / Premium SP1 ou suivant ;
- Microsoft Small Business Server 2008 Standard / Premium ;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Server 2008 Core R2 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Hyper-V Server 2008 R2 SP1 ou suivant ;
- Microsoft Small Business Server 2011 Essentials / Standard ;
- Microsoft Windows MultiPoint™ Server 2011 Standard / Premium ;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter ;
- Microsoft Windows MultiPoint™ Server 2012 Standard / Premium ;
- Windows Storage Server 2012 ;
- Windows Hyper-V Server 2012 ;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2012 Core R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Storage Server 2012 R2 ;
- Windows Hyper-V Server 2012 R2 ;
- Windows Server 2016 Essentials / Standard / Datacenter ;
- Windows Server 2016 MultiPoint ;
- Windows Server 2016 Core Standard / Datacenter ;
- Microsoft Windows MultiPoint™ Server 2016 ;
- Windows Storage Server 2016 ;
- Windows Hyper-V Server 2016 ;
- Windows Server 2019 Essentials / Standard / Datacenter ;
- Windows Server 2019 Core ;
- Windows Storage Server 2019 ;
- Windows Hyper-V Server 2019.

Les systèmes d'exploitation suivants ne sont plus pris en charge par Microsoft Windows : Windows Server 2003 Standard/Enterprise/Datacenter SP2, Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 32 bits, 64 bits. Des limitations risquent d'affecter l'assistance technique des serveurs exécutant ces systèmes d'exploitation du côté de Kaspersky Lab.

Vous pouvez installer Kaspersky Security for Windows Server sur un des serveurs de terminaux suivants :

- Microsoft Remote Desktop Services sur la base de Windows Server 2008 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2008 R2 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2012 R2 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2016 ;
- Microsoft Remote Desktop Services sur la base de Windows Server 2019 ;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15 ;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

Kaspersky Security for Windows Server est compatible avec les versions suivantes de Kaspersky Security Center :

- Kaspersky Security Center 10.4 ;
- Kaspersky Security Center 10.5 ;
- Kaspersky Security Center 11.

## Configuration requise pour le périphérique de stockage NAS protégé

Kaspersky Security for Windows Server peut être utilisé pour la protection des périphériques de stockage NAS suivants :

- NetApp sous un des systèmes d'exploitation suivants :
  - Data ONTAP 7.x et Data ONTAP 8.x en mode 7-mode ;
  - Data ONTAP 8.2.1 en mode cluster-mode ;
  - Data ONTAP 9.0 en mode cluster-mode ;
  - Data ONTAP 9.1 en mode cluster-mode ;
  - Data ONTAP 9.2 en mode cluster-mode ;
  - Data ONTAP 9.3 en mode cluster-mode ;
  - Data ONTAP 9.4 en mode cluster-mode.
- Dell™ EMC™ Celerra™ / VNX™ avec la configuration logicielle suivante :
  - Système d'exploitation EMC DART 6.0.36 ou suivant ;
  - Celerra Antivirus Agent (CAVA) 4.5.2.3 ou supérieure.
- Dell EMC Isilon™ sous le système d'exploitation OneFS™ 7.0 ou suivant ;
- Hitachi HNAS (ICAP, RPC) :

- 12.0 ou suivant pour l'intégration via ICAP ;
- 11.2 ou suivant pour l'intégration via RPC.
- Série IBM System Storage N ;
- Oracle® ZFS Storage Appliance ;
- Dell NAS sur la plateforme Dell Compellent™ FS8600 :
  - FluidFS 6.x ;
  - FluidFS 5.x.
- HPE 3PAR avec File Persona 3.3.1 :
  - Contrôleur de fichiers HPE 3PAR STORESERV ;
  - Stockage HPE 3PAR STORESERV 7000c, 8000, 9000, 20000.

## Configuration requise pour l'ordinateur sur lequel la Console de l'application est installée

### Configuration matérielle requise pour l'ordinateur

Mémoire vive recommandée : 128 Mo minimum.

Espace disque disponible : 30 Mo.

### Configuration logicielle requise pour l'ordinateur

Vous pouvez installer la console de l'application sur un ordinateur tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows.

L'installation et l'utilisation de la console de l'application sur l'ordinateur requièrent Microsoft Windows Installer 3.1.

Vous pouvez installer la Console de l'application sur un ordinateur tournant sous une des versions 32 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Windows XP Professional SP2 ou suivant ;
- Microsoft Windows Vista® ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8.1 ;
- Microsoft Windows 10 ;
- Windows 10 Redstone 1 ;
- Windows 10 Redstone 2 ;
- Windows 10 Redstone 3 ;

- Windows 10 Redstone 4 ;
- Windows 10 Redstone 5 ;
- Windows 10 Redstone 6.

Vous pouvez installer la Console de l'application sur un ordinateur tournant sous une des versions 64 bits d'un système d'exploitation Microsoft Windows suivants :

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou suivant ;
- Windows Server 2008 Core / Standard / Enterprise / Datacenter SP1 ou suivant ;
- Microsoft Small Business Server 2008 Standard / Premium ;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 ou suivant ;
- Windows Hyper-V Server 2008 R2 SP1 ou suivant ;
- Microsoft Small Business Server 2011 Essentials / Standard ;
- Microsoft Windows MultiPoint Server 2011 Standard / Premium ;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter ;
- Microsoft Windows MultiPoint Server 2012 Standard / Premium ;
- Windows Storage Server 2012 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Storage Server 2012 R2 ;
- Windows Hyper-V Server 2012 ;
- Windows Hyper-V Server 2012 R2 ;
- Windows Server 2016 Essentials / Standard / Datacenter ;
- Microsoft Windows MultiPoint Server 2016 ;
- Windows Storage Server 2016 Essentials / Standard / Datacenter ;
- Windows Server 2019 Essentials / Standard / Datacenter ;
- Windows Storage Server 2019 ;
- Microsoft Windows XP Professional Edition SP2 ou suivant ;
- Microsoft Windows Vista ;
- Microsoft Windows 7 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8.1 ;
- Microsoft Windows 10 ;
- Windows 10 Redstone 1 ;
- Windows 10 Redstone 2 ;
- Windows 10 Redstone 3 ;
- Windows 10 Redstone 4 ;

- Windows 10 Redstone 5 ;
- Windows 10 Redstone 6.

## Exigences fonctionnelles et restrictions

Cette section décrit des exigences fonctionnelles supplémentaires et les restrictions existantes pour les modules de Kaspersky Security for Windows Server.

### Dans cette section

Installation et désinstallation .....	<a href="#">31</a>
Protection du trafic .....	<a href="#">31</a>
Moniteur d'intégrité des fichiers .....	<a href="#">32</a>
Gestion du pare-feu .....	<a href="#">33</a>
Autres restrictions .....	<a href="#">34</a>

## Installation et désinstallation

- Lors de l'installation de l'application, un avertissement s'affiche si le nouveau chemin du dossier d'installation de Kaspersky Security for Windows Serveur contient plus de 150 caractères. L'avertissement n'affecte pas le processus d'installation : Kaspersky Security for Windows Server s'installe et s'exécute correctement.
- Pour installer le module de prise en charge du protocole SNMP, il faut redémarrer le service SNMP si celui-ci est en cours d'exécution.
- Pour installer et utiliser Kaspersky Security for Windows Server sur l'appareil administré par le système d'exploitation intégré, le composant Gestionnaire de filtre doit être installé.
- Il est impossible d'installer les outils d'administration de Kaspersky Security for Windows Server via les stratégies de groupe Microsoft Active Directory.
- Lors de l'installation de l'application sur des ordinateurs tournant sous des versions antérieures du système d'exploitation qui ne peuvent pas recevoir les mises à jour régulières, il convient de vérifier les certificats racine suivants : DigiCert Assured ID Root CA, DigiCert\_High\_Assurance\_EV\_Root\_CA et DigiCertAssuredIDRootCA. L'absence des certificats indiqués peut entraîner un mauvais fonctionnement de l'application. Il est conseillé d'installer les certificats indiqués de n'importe quelle manière possible.

## Protection du trafic

- Le composant est disponible uniquement sur les serveurs tournant sous des systèmes d'exploitation postérieurs à Microsoft Windows Server 2008 R2.
- Il est impossible d'analyser le trafic quand les connexions Internet sont établies avec un token de chiffrement.
- Il est déconseillé d'inclure le trafic VPN dans la zone de protection (port 1723).

- L'utilisation d'adresses IP au format IPv6 n'est pas pris en charge.
- L'application considère les certificats auto-signés comme des certificats non valide et bloque ces connexions si la case **Ne pas faire confiance aux serveurs Internet dotés d'un certificat non valide** est cochée dans les paramètres de la tâche.
- L'application traite seulement les paquets TCP.
- La protection contre les menaces email n'analyse pas le trafic sortant.
- Il est conseillé d'installer le Plug-in d'administration avant de déployer le module Protection du trafic car l'Agent d'administration du Serveur d'administration détecte ce module lors de la connexion à l'application. Si Protection du trafic était installé et si la tâche a démarré avant l'installation du Plug-in d'administration, relancez la tâche Protection du trafic.
- La Protection du trafic ne prend pas en charge Yandex.Disk, Dropbox.
- Restrictions VPN : des problèmes peuvent se présenter en cas d'utilisation via les protocoles de connexion Microsoft VPN.
- Si l'installation est réalisée via Kaspersky Security Center en mode Intercepteur de pilote, la Protection du trafic bloque la connexion entre la Microsoft Management Console (ci-après MMS) et le Serveur d'administration de Kaspersky Security Center car ce genre de connexion utilise un certificat bloqué.
- Le module bloque la connexion aux sites qui utilisent d'anciennes technologies de génération de certificats racine, par exemple sha1 certificate.
- La valeur de **Ne pas analyser les objets de plus de (Mo)** ne peut être supérieure à 100 Mo. Si la valeur saisie est grande et si la connexion Internet est lente, il pourrait y avoir des difficultés au niveau de la réception de gros fichiers. La valeur recommandée est de 20 Mo.
- L'application considère les connexions HTTPS comme dangereuses et les bloque si les conditions suivantes sont remplies :
  - La tâche est exécutée en mode **Intercepteur de pilote**.
  - Le trafic est redirigé depuis des appareils externes.
  - Les appareils depuis lesquels le trafic est redirigé sont protégés par Kaspersky Security for Windows Server et la tâche prédéfinie Protection du trafic a été exécutée au moins une fois.

Nous déconseillons l'utilisation du mode **Redirection** pour analyser le trafic redirigé depuis des ordinateurs externes : outre les faux positifs cités ci-dessus, cette configuration peut augmenter la charge sur le serveur et réduire les performances de l'application.

## Moniteur d'intégrité des fichiers

Par défaut, le Moniteur d'intégrité des fichiers ne surveille pas les modifications dans les dossiers système ou dans les fichiers d'entretien du système de fichier afin d'éviter que les informations relatives aux modifications de fichier de routine, réalisées en permanence par le système d'exploitation, n'entre dans les rapports de tâche. L'utilisateur ne peut pas inclure manuellement ces dossiers dans la zone de monitoring.

Les dossiers/fichiers suivants sont exclus de la zone de monitoring :

- Fichiers d'entretien NTFS porteurs de l'identifiant de 0 à 33
- "%SystemRoot%\Prefetch\"
- "%SystemRoot%\ServiceProfiles\LocalService\AppData\Local\"
- "%SystemRoot%\System32\LogFiles\Scm\"
- "%SystemRoot%\Microsoft.NET\Framework\v4.0.30319\"
- "%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\"
- "%SystemRoot%\Microsoft.NET\"
- "%SystemRoot%\System32\config\"
- "%SystemRoot%\Temp\"
- "%SystemRoot%\ServiceProfiles\LocalService\"
- "%SystemRoot%\System32\winevt\Logs\"
- "%SystemRoot%\System32\wbem\repository\"
- "%SystemRoot%\System32\wbem\Logs\"
- "%ProgramData%\Microsoft\Windows\WER\ReportQueue\"
- "%SystemRoot%\SoftwareDistribution\DataStore\"
- "%SystemRoot%\SoftwareDistribution\DataStore\Logs\"
- "%ProgramData%\Microsoft\Windows\AppRepository\"
- "%ProgramData%\Microsoft\Search\Data\Applications\Windows\"
- "%SystemRoot%\Logs\SystemRestore\"
- "%SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\"

L'application exclut les dossiers du niveau supérieur.

Le module ne surveille pas les modifications de fichiers qui contournent le système de fichiers ReFS/NTFS (les modifications de fichier sont réalisées via BIOS, LiveCD, etc.).

## Gestion du pare-feu

- L'utilisation des adresses IP au format IPv6 n'est pas prise en charge quand la zone d'application de la règle ne contient qu'une seule adresse.
- Les règles prédéfinies de stratégie du Pare-feu permettent d'exécuter des scénarios d'interaction de base entre les ordinateurs locaux et le Serveur d'administration. Pour utiliser toutes les fonctions de Kaspersky Security Center, il faut configurer les règles pour les ports manuellement. Les informations relatives aux numéros de port, aux protocoles et à leurs fonctions sont reprises dans la Banque de solution de Kaspersky Security Center (ID de l'article : 9297).
- L'application ne contrôle pas les modifications des règles du Pare-feu Windows et des groupes de règles lors des requêtes ponctuelles de la tâche Gestion du Pare-feu si ces règles n'ont pas été ajoutés à la configuration de la tâche lors de l'installation de l'application. Pour mettre à jour l'état et inclure ces règles, il faut redémarrer la tâche Gestion du Pare-feu.



- Pour les systèmes d'exploitation Microsoft Windows Server 2008 et suivants : il faut démarrer le service Windows Firewall (démarré par défaut) avant d'installer le module Gestion du Pare-feu.
- Quand la tâche Gestion du Pare-feu est lancée, les types de règles suivants sont automatiquement supprimés des paramètres du pare-feu du système d'exploitation :
  - règles d'interdiction ;
  - règles de surveillance du trafic sortant.

## Autres restrictions

### Analyse à la demande, Protection des fichiers en temps réel :

- L'analyse des appareils MTP connectés n'est pas disponible.
- L'analyse des archives n'est pas disponible sans l'analyse des archives SFX : si l'analyse des archives est activée dans les paramètres de protection de Kaspersky Security for Windows Server, l'application analyse automatiquement les objets dans les archives et les archives SFX. L'analyse des archives SFX sans l'analyse des archives est disponible.

### Commande et diagnostic de l'ordinateur :

- La zone de protection de la tâche Contrôle des périphériques inclut les appareils connectés par MTP si un ordinateur protégé tourne sous Microsoft Windows Server 2008 R2 ou suivant.
- La tâche d'inspection des journaux détecte uniquement les signes d'attaque Kerberos potentielle (MS14-068) sur les ordinateurs tournant sous Windows Server 2008 ou suivants en tant que contrôleur de domaine avec mises à jour installées.

### Licence :

- L'activation de l'application à l'aide de la clé dans l'assistant d'installation n'est pas disponible si la clé est stockée sur le disque créé à l'aide de la commande SUBST ou si le chemin d'accès réseau du fichier clé est défini.

### Mises à jour :

- Après l'installation des mises à jour critiques des modules de Kaspersky Security for Windows Server, l'icône de l'application est masquée par défaut.
- KLRAMDISK n'est pas pris en charge sur les ordinateurs tournant sous Windows XP ou Windows 2003.

### Interface :

- Si vous utilisez le filtre dans la Console de l'application dans la Quarantaine, la Sauvegarde, le journal d'audit système ou le Journal d'exécution de la tâche, le cas doit être maintenu.
- Vous pouvez utiliser un seul masque et uniquement à la fin du chemin, lors de la configuration de la protection ou de la zone d'analyse dans la Console de l'application. Exemples d'utilisation correcte du masque : "C:\Temp\Temp\*" ou "C:\Temp\Temp???.doc" ou "C:\Temp\Temp\*.doc". La restriction ne touche pas la configuration de la zone de confiance.

### Sécurité :

- Si la fonction de contrôle des comptes utilisateur est activée dans les paramètres du système d'exploitation, un compte utilisateur doit appartenir au groupe KAVWSEE Administrators pour pouvoir ouvrir la Console de l'application d'un double clic sur l'application de l'icône dans la zone de notification de la barre d'état. Dans un autre cas, il sera nécessaire de vous connecter en tant qu'utilisateur. Cette action est autorisée pour

ouvrir l'interface de diagnostic compacte ou le composant logiciel enfichable ou MMC.

- Il est impossible de désinstaller l'application via la fenêtre "Programmes et caractéristiques" de Microsoft Windows si le contrôle du compte utilisateur est activé.

#### **Intégration à Kaspersky Security Center :**

- Le Serveur d'administration vérifie la validité des mises à jour de la base de données lors de la réception des paquets de mise à jour et avant d'envoyer ces mises à jour aux ordinateurs du réseau. Le Serveur d'administration ne vérifie pas la validité des mises à jour des modules de l'application.
- Assurez-vous que les cases requises sont cochées dans les paramètres Interaction avec le Serveur d'administration quand vous utilisez des composants qui transmettent les données modifiées dynamiquement à Kaspersky Security Center à l'aide des listes réseau (Quarantaine, Sauvegarde, ordinateurs bloqués).

#### **Protection contre les exploits :**

- La Protection contre les exploits n'est pas disponible si les bibliothèques apphelp.dll ne sont pas chargées dans la configuration d'environnement actuelle.
- Le composant Protection contre les exploits est incompatible avec l'utilitaire EMET de Microsoft tournant sous le système d'exploitation Microsoft Windows 10 : Kaspersky Security for Windows Server bloque EMET si le composant Protection contre les exploits est en cours d'installation sur un ordinateur hébergeant EMET.

#### **Protection contre le chiffrement pour NetApp :**

- La Protection contre le chiffrement ne peut être offerte aux périphériques de stockage réseau tournant sous de nouveaux systèmes d'exploitation (ONTAP 9 et suivant) si des conteneurs FlexGroup sont utilisés pour ces serveurs.
- La fonction de détection des menaces contre les fichiers sur les périphériques de stockage réseau NetApp en mode 7 est limitée.
- La Protection contre le chiffrement pour NetApp est disponible uniquement en mode cluster.
- Un serveur peut utiliser uniquement une interface réseau et une seule adresse IPv4.

**Liste des ordinateurs bloqués :** exécutée en continue lorsque la Protection contre le chiffrement ou la Protection des fichiers en temps réel est activée.

#### **Protection ICAP des stockages réseau connectés :**

- La gestion du contenu des stockages protégés dépend des paramètres du stockage. Par exemple, il est impossible de supprimer les fichiers infectés détectés si le stockage n'autorise pas cette action.
- Le stockage HPE 3PAR fonctionne uniquement en mode d'accès au bloc.
- Si une règle d'exclusion pour objets not-a-virus est active dans la zone de confiance, elle est aussi appliquée à la tâche Protection ICAP des stockages réseau connectés.

**Protection RPC des stockages réseau connectés :** Active Directory est requis en mode cluster.

**Utilisation du KSN :** Pour Windows Vista et les versions précédentes des systèmes d'exploitation Windows, ce composant ne prend pas en charge les statistiques pour la protection contre les menaces Internet et la protection contre les menaces email.

# Installation et suppression de l'application

Cette section explique pas à pas la procédure d'installation et de désinstallation de Kaspersky Security for Windows Server.

## Contenu du chapitre

Codes des composants logiciel de Kaspersky Security for Windows Server pour le service Windows Installer .....	<a href="#">36</a>
Modifications introduites dans le système après l'installation de Kaspersky Security for Windows Server .....	<a href="#">40</a>
Processus de Kaspersky Security for Windows Server .....	<a href="#">43</a>
Paramètres d'installation et de désinstallation et options de ligne de commande correspondantes pour le service Windows Installer .....	<a href="#">44</a>
Journaux d'installation et de désinstallation de Kaspersky Security for Windows Server .....	<a href="#">47</a>
Planification de l'installation .....	<a href="#">47</a>
Installation et suppression de l'application à l'aide de l'Assistant .....	<a href="#">50</a>
Installation et suppression de l'application via la ligne de commande .....	<a href="#">65</a>
Installation et suppression de l'application via Kaspersky Security Center .....	<a href="#">71</a>
Installation et suppression via les stratégies de groupe Active Directory .....	<a href="#">76</a>
Vérification des fonctions de Kaspersky Security for Windows Server.Utilisation du virus d'essai EICAR .....	<a href="#">78</a>

## Codes des composants logiciel de Kaspersky Security for Windows Server pour le service Windows Installer

Par défaut, les fichiers `\server\ks4ws_x86(x64).msi` sont prévus pour installer tous les composants de Kaspersky Security for Windows Server. Vous pouvez installer ces composants en les incluant dans une installation personnalisée.

Les fichiers `\client\ks4wstools_x86(x64).msi` installent tous les composants logiciels de la sélection "Outils d'administration".

Les rubriques suivantes indiquent les codes des composants de Kaspersky Security for Windows Server pour le service Windows Installer. Vous pouvez utiliser ces codes dans le but de définir la liste des composants à installer lors de l'installation de Kaspersky Security for Windows Server via la ligne de commande.

### Dans cette section

Composants logiciels de Kaspersky Security for Windows Server .....	<a href="#">37</a>
Ensemble des "Outils d'administration" des composants logiciels .....	<a href="#">39</a>

## Composants logiciels de Kaspersky Security for Windows Server

Le tableau ci-après contient les codes et la description des composants logiciels de Kaspersky Security for Windows Server.

Tableau 3. Description des composants logiciels de Kaspersky Security for Windows Server

Composant	Code	Fonction exécutée
Fonction principale	Core	Ce composant contient une sélection de fonctions de base de l'application et garantit leur fonctionnement.
Contrôle du lancement des applications	AppCtrl	Ce composant surveille les tentatives de lancement des applications par les utilisateurs et autorise ou interdit le lancement des applications conformément aux règles du Contrôle du lancement des applications indiquées. Le composant intervient dans la tâche Contrôle du lancement des applications.
Contrôle des périphériques	DevCtrl	Ce composant surveille les tentatives de connexion de périphérique de stockage de masse sur un serveur protégé et autorise ou non leur utilisation en fonction des règles de contrôle des périphériques. Le composant intervient dans la tâche Contrôle des périphériques.
Protection du trafic	WebGW	Ce composant traite le trafic Internet (y compris le trafic obtenu via les services de messagerie) et intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informatiques connues et autres sur le serveur protégé.
Protection antivirus	AVProtection	Ce composant garantit la protection antivirus et reprend les composants suivants : Analyse à la demande ; Protection des fichiers en temps réel.
Analyse à la demande	Ods	Ce composant installe les fichiers système de Kaspersky Security for Windows Server et permet d'exécuter les tâches d'analyse à la demande (analyse des objets du serveur protégé exécutée à la demande). Si lors de l'installation de Kaspersky Security for Windows Server via la ligne de commande vous désignez d'autres composants de Kaspersky Security for Windows Server sans le composant Core, celui-ci sera installé automatiquement.
Protection des fichiers en temps réel	Oas	Ce composant réalise l'analyse antivirus des fichiers sur le serveur protégé lorsque ces fichiers sont sollicités. Le composant exécute la tâche Protection des fichiers en temps réel.

Composant	Code	Fonction exécutée
Protection contre le chiffrement	AntiCryptor	Ce composant remplit la liste des hôtes bloqués avec les noms des appareils distants qui affichent une activité malveillante. Il met en oeuvre la tâche de protection contre le chiffrement.
Monitoring des scripts	ScriptChecker	Ce composant analyse le code des scripts créés à l'aide des technologies Microsoft Windows Script Technologies. L'analyse a lieu en cas de tentative d'exécution d'un script. Ce composant met en oeuvre la tâche Monitoring des scripts.
Utilisation de Kaspersky Security Network	Ksn	Ce composant offre une protection sur la base des technologies cloud de Kaspersky Lab. Le composant exécute la tâche Utilisation du KSN (envoi de requêtes au Service Kaspersky Security Network et réception des conclusions de ce même Service Kaspersky Security Network).
Moniteur d'intégrité des fichiers	Fim	Ce composant permet de consigner les opérations réalisées sur les fichiers dans la zone de monitoring sélectionnée. Le composant intervient dans la tâche Moniteur d'intégrité des fichiers.
Protection contre les exploits	AntiExploit	Ce composant garantit l'administration des paramètres de la protection des processus dans la mémoire du serveur protégé.
Gestion du pare-feu	Firewall	Ce composant permet d'administrer le pare-feu Windows via l'interface utilisateur graphique de Kaspersky Security for Windows Server. Le composant intervient dans la tâche Gestion du pare-feu.
Module d'intégration de l'Agent d'administration de Kaspersky Security Center	AKIntegration	Ce composant garantit la connexion entre Kaspersky Security for Windows Server et l'Agent d'administration Kaspersky Security Center. Vous pouvez installer ce composant sur le serveur protégé si vous avez l'intention d'administrer l'application via Kaspersky Security Center.
Inspection des journaux	LogInspector	Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.
Protection RPC des stockages réseau connectés	RPCProt	Ce composant protège les périphériques de stockage NAS connectés via RPC (par exemple les périphériques de stockage NAS de NetApp) contre les virus et autres menaces informatiques qui se propagent dans le serveur via l'échange de fichiers.

Composant	Code	Fonction exécutée
Protection ICAP des stockages réseau connectés	ICAPProt	Ce composant protège les stockages réseau connectés via ICAP (par exemple EMC Isilon) contre les virus et autres menaces informatiques qui se propagent dans le serveur via l'échange de fichiers.
Protection contre le chiffrement pour NetApp	AntiCryptorNAS	Ce composant protège les dossiers des périphériques de stockage NAS contre le chiffrement malveillant. En cas de détection d'un chiffrement malveillant, Kaspersky Security for Windows Server interdit l'accès aux dossiers du périphérique de stockage NAS protégé.
Sélection de compteurs de performance de l'application "System Monitor"	PerfMonCounters	Le composant installe la sélection de compteurs de performance de l'application "System Monitor". Ces compteurs de performance permettent de mesurer les performances de Kaspersky Security for Windows Server et de localiser les éventuels goulots d'étranglement sur l'ordinateur lors de l'utilisation de Kaspersky Security for Windows Server avec d'autres applications.
Prise en charge du protocole SNMP	SnmpSupport	Le composant publie les compteurs et les pièges de Kaspersky Security for Windows Server via le service Simple Network Management Protocol (SNMP) sur Microsoft Windows. Ce composant ne peut être installé sur le serveur protégé que si Microsoft SNMP est installé sur ce même ordinateur.
Icône de Kaspersky Security for Windows Server dans la zone de notification	TrayApp	Le composant affiche l'icône de Kaspersky Security for Windows Server dans la zone de notification de la barre des tâches du serveur protégé. L'icône de Kaspersky Security for Windows Server affiche l'état de la protection du serveur, permet d'ouvrir la Console de l'application dans Microsoft Management Console (si elle est installée) et la fenêtre <b>A propos de l'application</b> .

## Ensemble des "Outils d'administration" des composants logiciels

Le tableau suivant contient les codes et les descriptions des composants logiciels de la sélection "Outils d'administration".

Tableau 4. Description des composants logiciels de la sélection "Outils d'administration"

Composant	Code	Fonctions du composant
Composant logiciel enfichable de Kaspersky Security for Windows Server	MmcSnapin	Le composant installe le composant logiciel enfichable Microsoft Management Console pour l'administration via la Console de Kaspersky Security for Windows Server.  Si lors de l'installation de la sélection "Outils d'administration" via la ligne de commande vous désignez d'autres composants de la sélection sans le composant MmcSnapin, celui-ci sera installé automatiquement.

Composant	Code	Fonctions du composant
Aide	Help	Il s'agit d'un fichier chm de l'aide ; il est enregistré dans le dossier qui contient les fichiers des outils d'administration de Kaspersky Security for Windows Server. Vous pouvez ouvrir le fichier d'aide via le menu <b>Démarrer</b> ou via la touche <b>F1</b> de la fenêtre ouverte de la console de l'application.
Documentation	Help	Kaspersky Security for Windows Server ajoute un raccourci vers le site Internet de Kaspersky Lab qui propose le Manuel d'implantation pour la protection des stockages réseau. Le Manuel de l'administrateur est disponible au format PDF. Le raccourci est disponible dans le menu <b>Démarrer</b> .

## Modifications introduites dans le système après l'installation de Kaspersky Security for Windows Server

Lors de l'installation de Kaspersky Security for Windows Server et de la sélection d'"Outils d'administration" (y compris la console de l'application), le service Windows Installer procède aux modifications suivantes sur le serveur protégé :

- création des dossiers de Kaspersky Security for Windows Server sur le serveur protégé et sur le serveur sur lequel la console de l'application est installée ;
- enregistrement des services Kaspersky Security for Windows Server ;
- création d'un groupe d'utilisateurs de Kaspersky Security for Windows Server.
- Les clés de Kaspersky Security for Windows Server sont enregistrées dans la base de registres.

Ces modifications sont décrites ci-dessous.

### Dossier de Kaspersky Security for Windows Server sur un serveur protégé

Suite à l'installation de Kaspersky Security for Windows Server, les dossiers suivants sont créés sur un serveur protégé :

- Le dossier d'installation par défaut de Kaspersky Security for Windows Server contenant les fichiers exécutables de Kaspersky Security for Windows Server dépend de la version (bits) du système d'exploitation. Par conséquent, les dossiers d'installation par défaut sont les suivants :
  - Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\
  - Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\
- Les fichiers Management Information Base (MIB) contenant une description des compteurs et les pièges publiés par Kaspersky Security for Windows Server selon le protocole SNMP :
  - %Kaspersky Security for Windows Server%\mibs
- Version 64 bits des fichiers exécutables de Kaspersky Security for Windows Server (le dossier est créé



uniquement lors de l'installation de Kaspersky Security for Windows Server sur une version 64 bits de Microsoft Windows) :

- %Kaspersky Security for Windows Server%\x64
- Fichiers de service de Kaspersky Security for Windows Server :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Data\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Settings\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Dskm\
- Fichiers contenant les paramètres pour les sources de mise à jour :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\
- Mises à jour des bases de données et des modules logiciels récupérés à l'aide de la tâche Copie des mises à jour (le dossier est créé à la première réception des mises à jour à l'aide de la tâche Copie des mises à jour) :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\Distribution\
- Journaux d'exécution de la tâche et journal d'audit système :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\
- Ensemble de bases de données utilisées actuellement :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Current\
- Copies de sauvegarde des bases ; elles sont écrasées à chaque mise à jour des bases de données :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Backup\
- Fichiers temporaires créés lors de l'exécution des tâches de mise à jour :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Temp\
- Objets en quarantaine (dossier par défaut) :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\
- Objets dans la sauvegarde (dossier par défaut) :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\
- Objets restaurés de la Sauvegarde ou de la quarantaine (dossier par défaut pour les objets restaurés) :
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\

### Dossier créé lors de l'installation de la Console de l'application

Les dossiers d'installation par défaut de la Console de l'application contenant les fichiers "Outils d'administration" dépendent de la version (bits) du système d'exploitation. Par conséquent, les dossiers d'installation par défaut sont les suivants :

- Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\
- Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\

### Services de Kaspersky Security for Windows Server

Les services de Kaspersky Security for Windows Server suivants sont lancés sous le compte utilisateur Système local (SYSTEM) :

- Service Kaspersky Security (KAVFS) : service essentiel de Kaspersky Security for Windows Server qui gère les tâches et les flux de travail de Kaspersky Security for Windows Server.
- Service Kaspersky Security Management (KAVFSGT) : ce service est destiné à l'administration de l'application Kaspersky Security for Windows Server via la Console de l'application.
- Service Kaspersky Security Exploit Prevention : service qui agit en tant qu'intermédiaire de communication des paramètres de sécurité aux agents de sécurité externes et de réception des données relatives aux événements de sécurité.
- Service Kaspersky Security Script Checker (KAVFSSCS) – ce service est lancé en même temps que la tâche Monitoring des scripts et permet de contrôler l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies.

### Groupe Kaspersky Security for Windows Server

Administrateurs KAVWSEE désigne un groupe sur le serveur protégé dont les utilisateurs ont un accès total au service Kaspersky Security Management et à toutes les fonctions de Kaspersky Security for Windows Server.

### Clés de la base de registres système

L'installation de Kaspersky Security for Windows Server s'accompagne de la création des clés de la base de registres système suivantes :

- Propriétés de Kaspersky Security for Windows Server :  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Paramètres du journal des événements de Kaspersky Security for Windows Server (journal des événements de Kaspersky) :  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Propriétés du service d'administration de Kaspersky Security for Windows Server :  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Paramètres des compteurs de performance :
  - Sur la version 32 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - Sur la version 64 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Paramètres du composant « prise en charge du protocole SNMP » :

- Sur la version 32 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\SnmpAgent]
- Sur la version 64 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]
- Paramètres du fichier dump :
  - Sur la version 32 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump]
  - Sur la version 64 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump]
- Paramètres du fichier de trace :
  - Sur la version 32 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\Trace]
  - Sur la version 64 bits de Microsoft Windows :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Trace]
- Configuration des tâches et des fonctions de l'application :  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment]

## Processus de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server lance les processus décrits dans le tableau ci-dessous.

Tableau 5. Processus de Kaspersky Security for Windows Server

Nom du fichier	Fonction
kavswp.exe	Flux de travail de Kaspersky Security for Windows Server
kavtray.exe	Processus de l'icône dans la barre d'état système
kavsmui.exe	Composant Interface de diagnostic compacte
kavshell.exe	Processus de l'utilitaire de la ligne de commande
kavsrcn.exe	Processus d'administration à distance Kaspersky Security for Windows Server
kavfs.exe	Processus du Service Kaspersky Security
kavsgt.exe	Processus du Service Kaspersky Security Management
kavfswh.exe	Processus du service Kaspersky Security Exploit Prevention Management
kavfsscs.exe	Service Kaspersky Security Script Checker

## Paramètres d'installation et de désinstallation et options de ligne de commande correspondantes pour le service Windows Installer

Cette section décrit les paramètres d'installation et de désinstallation de Kaspersky Security for Windows Server ainsi que leur valeur par défaut. Elle renseigne également les arguments pour modifier les valeurs des paramètres d'installation et leurs valeurs possibles. Vous pouvez utiliser ces arguments avec les arguments standard de l'instruction `msiexec` du service Windows Installer lors de l'installation de Kaspersky Security for Windows Server via la ligne de commande.

### Paramètres de d'installation et options de ligne de commande dans Windows Installer

- Acceptation des termes du Contrat de licence utilisateur final : il faut accepter les dispositions pour installer Kaspersky Security for Windows Server.

Les valeurs qui peuvent être attribuées au paramètre `EULA=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : vous n'acceptez pas les termes du Contrat de licence utilisateur final.
- 1 : vous acceptez les termes du Contrat de licence utilisateur final.
- Acceptation des termes de la Politique de confidentialité : il faut accepter les dispositions pour installer Kaspersky Security for Windows Server.

Les valeurs qui peuvent être attribuées au paramètre `PRIVACYPOLICY=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : vous n'acceptez pas les termes de la Politique de confidentialité (valeur par défaut).
- 1 : vous acceptez les termes de la Politique de confidentialité.
- Installation de Kaspersky Security for Windows Server avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux.

Les valeurs qui peuvent être attribuées au paramètre `PRESCAN=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : ne pas effectuer d'analyse préliminaire des processus actifs et des secteurs d'amorçage des disques locaux pendant l'installation (valeur par défaut).
- 1 : effectuer une analyse préliminaire des processus actifs et des secteurs d'amorçage des disques locaux pendant l'installation.
- Dossier d'installation dans lequel les fichiers de Kaspersky Security for Windows Server vont être enregistrés lors de son installation. Vous pouvez indiquer un autre dossier.

Les valeurs par défaut attribuées au paramètres `INSTALLDIR=<chemin d'accès complet au dossier>` via la ligne de commande sont les suivantes :

- Kaspersky Security for Windows Server : `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server`
- Outils d'administration : `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools`
- Sur la version 64 bits de Microsoft Windows : `%ProgramFiles(x86)%`
- La tâche Protection des fichiers en temps réel démarre immédiatement après le démarrage de Kaspersky

Security for Windows Server. Activez ce paramètre pour démarrer la Protection des fichiers en temps réel et le Monitoring des scripts lorsque Kaspersky Anti-Virus for Windows Server démarre (recommandé).

Les valeurs qui peuvent être attribuées au paramètre `RUNRTP=<valeur>` dans la ligne de commande sont les suivantes :

- 1 : lancement (valeur par défaut).
- 0 : ne pas démarrer.
- Exclusions de la protection recommandées par Microsoft Corporation. Dans la tâche Protection des fichiers en temps réel sont exclus de la zone de protection les objets du serveur dont l'exclusion est recommandée par Microsoft Corporation. Certaines applications sur le serveur peuvent devenir instables lorsqu'une application antivirus intercepte ou modifie les fichiers auxquels ces applications utilisent. Ainsi, Microsoft Corporation inclus certains logiciels chargés du contrôle des domaines dans cette catégorie.

Les valeurs qui peuvent être attribuées au paramètre `ADDMSEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

- 1 : exclusion (valeur par défaut).
- 0 : ne pas exclure.
- Objets exclus de la zone de protection conformément aux recommandations de Kaspersky Lab. Dans la tâche Protection des fichiers en temps réel, les objets du serveur dont l'exclusion est recommandée par Kaspersky Lab sont exclus de la zone de protection.

Les valeurs qui peuvent être attribuées au paramètre `ADDKLEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

- 1 : exclusion (valeur par défaut).
- 0 : ne pas exclure.
- Autoriser les connexions à distance à la console de l'application. Par défaut, la connexion à distance à la console de l'application installée sur le serveur protégé n'est pas autorisée. Vous pouvez autoriser cette connexion pendant l'installation. Kaspersky Security for Windows Server crée les règles d'autorisation pour le processus `kavfsgt.exe` sur le protocole TCP pour tous les ports.

Les valeurs qui peuvent être attribuées au paramètre `ALLOWREMOTECON=<valeur>` dans la ligne de commande sont les suivantes :

- 1 : autoriser.
- 0 : interdire (valeur par défaut).
- Chemin d'accès au fichier clé. Par défaut, Windows Installer tente de trouver le fichier avec l'extension `.key` dans le dossier `\server` du kit de distribution. Si le dossier `\server` contient plusieurs fichiers clé, Windows Installer choisit le fichier clé qui possède la date de fin de validité la plus lointaine. Vous pouvez enregistrer au préalable le fichier clé dans le répertoire `\server` ou indiquer un autre chemin d'accès au fichier clé à l'aide du paramètre **Ajouter une clé**. Vous pouvez ajouter une clé après l'installation de Kaspersky Security for Windows Server à l'aide de l'outil d'administration que vous aurez choisi, par exemple via la console de l'application. Si vous n'ajoutez pas la clé de l'application lors de son installation, Kaspersky Security for Windows Server ne fonctionnera pas.

La valeur par défaut pour le paramètre `LICENSEKEYPATH=<nom du fichier clé>` est le nom du dossier `\server` dans le kit de distribution.

- Chemin d'accès au fichier de configuration. Kaspersky Security for Windows Server importe les paramètres depuis le fichier de configuration indiqué et créé dans l'application. Kaspersky Security for Windows Server n'importe pas les mots de passe contenus dans le fichier de configuration tels que les mots de passe des

comptes utilisateur de lancement de tâches ou les mots de passe de connexion au serveur proxy. Après l'importation des paramètres, vous devrez saisir tous les mots de passe manuellement. Si vous ne désignez pas le fichier de configuration, Kaspersky Security for Windows Server fonctionnera après l'installation selon les paramètres par défaut.

La valeur par défaut pour le paramètre `CONFIGPATH=<nom du fichier de configuration>` n'est pas définie.

- Autorisation des connexions de réseau pour la Console de l'application. Cette option permet d'installer Kaspersky Security for Windows Server sur un autre serveur. Grâce à la console de Kaspersky Security for Windows Server installée sur un autre ordinateur, vous pourrez administrer la protection d'un serveur à distance. Le port TCP 135 est ouvert dans le pare-feu de Microsoft Windows, les connexions réseau sont autorisées pour le fichier exécutable du processus d'administration à distance de Kaspersky Security for Windows Server `kavfsrcn.exe` et l'accès aux applications DCOM est ouvert. Une fois l'installation terminée, ajoutez les utilisateurs au groupe KAVWSEE Administrators pour leur permettre d'administrer l'application à distance si le serveur tourne sous Microsoft Windows Server 2008, et autorisez les connexions réseau au Service Kaspersky Security Management (`kavfsgt.exe`) sur le serveur. Vous pouvez lire des informations complémentaires sur la configuration quand la Console de Kaspersky Security for Windows Server est installée sur un autre ordinateur (cf. section "Configuration avancée après l'installation de la console de l'application sur un autre ordinateur" à la page [56](#)).

Les valeurs qui peuvent être attribuées au paramètre `ADDWFEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

- 1 : autoriser.
- 0 : interdire (valeur par défaut).
- Désactivation de la recherche d'une application non compatible. Ce paramètre permet d'activer ou de désactiver la recherche de logiciels incompatibles lors de l'installation de l'application en arrière-plan sur le serveur. Quelle que soit la valeur de ce paramètre, lors de l'installation de Kaspersky Security for Windows Server, l'application met toujours l'utilisateur en garde contre la présence d'autres versions de l'application sur le serveur.

Les valeurs qui peuvent être attribuées au paramètre `SKIPINCOMPATIBLESW=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : la recherche d'applications incompatibles a lieu (valeur par défaut).
- 1 : la recherche d'applications non compatibles n'a pas lieu.

### Paramètres de désinstallation et options de ligne de commande dans Windows Installer

- Restauration du contenu de la quarantaine.

Les valeurs qui peuvent être attribuées au paramètre `RESTOREQTN=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : suppression du contenu en quarantaine (valeur par défaut).
- 1 : restaurer le contenu de la quarantaine dans le dossier défini par le paramètre `RESTOREPATH`, dans le sous-dossier `\Quarantine`.
- Restauration du contenu de la Sauvegarde.

Les valeurs qui peuvent être attribuées au paramètre `RESTOREBCK=<valeur>` dans la ligne de commande sont les suivantes :

- 0 : suppression du contenu de la Sauvegarde (valeur par défaut).

- 1 : restaurer le contenu de la Sauvegarde dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \Backup.
- Saisie du mot de passe actif pour la confirmation de l'opération de désinstallation (lorsque la protection par mot de passe est activée).

La valeur par défaut pour le paramètre UNLOCK\_PASSWORD=<mot de passe défini> n'est pas définie.

- Dossier pour la restauration des objets. Les objets restaurés seront enregistrés dans le dossier spécifié. La valeur par défaut pour l'option RESTOREPATH=<chemin d'accès complet au dossier> de la ligne de commande est %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored.

## Journaux d'installation et de désinstallation de Kaspersky Security for Windows Server

Si vous installez ou désinstallez Kaspersky Security for Windows Server à l'aide de l'Assistant d'installation (Désinstallation), le service Windows Installer crée le journal d'installation (de désinstallation). Un fichier journal est enregistré sous le nom ks4ws\_install\_<uid>.log (où <uid> désigne un identifiant unique de 8 caractères) dans le dossier %temp% pour l'utilisateur sous le compte duquel le fichier setup.exe a été exécuté.

Si vous exécutez l'option **Modification ou suppression des Outils d'administration de Kaspersky Security 10.1.2 for Windows Server** de la Console de l'application ou Kaspersky Security for Windows Server à partir du menu **Démarrer**, le fichier journal ks4ws\_10.1\_maintenance.log est automatiquement créé dans le dossier %temp%.

Si vous installez ou désinstallez Kaspersky Security for Windows Server via la ligne de commande, le fichier journal d'installation n'est pas créé par défaut.

► *Pour installer Kaspersky Security for Windows Server et créer le fichier journal sur le disque C:\, exécutez l'instruction suivante :*

- `msiexec /i ks4ws_x86.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\ks4ws.log /qn EULA=1 PRIVACYPOLICY=1`

## Planification de l'installation

Cette section décrit la sélection d'outils d'administration de Kaspersky Security for Windows Server, les particularités de l'installation et de la suppression de Kaspersky Security for Windows Server à l'aide d'un assistant (cf. section "Installation et suppression de l'application à l'aide de l'assistant" à la page [50](#)), via la ligne de commande (cf. section "Installation et suppression de l'application via la ligne de commande" à la page [65](#)), via Kaspersky Security Center (cf. section "Installation et suppression de l'application via Kaspersky Security Center" à la page [71](#)) et via une stratégie de groupe Active Directory (cf. section "Installation et suppression via les stratégies de groupe Active Directory" à la page [76](#)).

Avant de lancer l'installation de Kaspersky Security for Windows Server, il convient de préparer les principales étapes de la procédure.



1. Définissez les outils d'administration que vous utiliserez pour administrer et configurer Kaspersky Security for Windows Server.
2. Déterminez les composants d'application requis à installer (cf. section "Composants logiciels de Kaspersky Security for Windows Server et leurs code pour le service Windows Installer" à la page [36](#)).
3. Sélectionnez le mode d'installation.

## Dans cette section

Sélection des outils d'administration.....	<a href="#">48</a>
Sélection du type d'installation .....	<a href="#">49</a>

## Sélection des outils d'administration

Définissez les outils d'administration que vous utiliserez pour la configuration des paramètres de Kaspersky Security for Windows Server et son administration. En guise d'outils d'administration de Kaspersky Security for Windows Server, vous pouvez choisir la console de l'application, l'utilitaire de ligne de commande ou la console d'administration de Kaspersky Security Center.

### Console de Kaspersky Security for Windows Server

La console de Kaspersky Security for Windows Server est un composant logiciel enfichable autonome qui est ajouté à la console Microsoft Management Console. Il est possible d'administrer Kaspersky Security for Windows Server via la console de l'application installée sur le serveur protégé ou sur tout autre ordinateur du réseau de l'organisation.

Dans une des consoles Microsoft Management Console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants logiciels enfichables Kaspersky Security for Windows Server afin de pouvoir administrer ainsi la protection de plusieurs serveurs sur lesquels Kaspersky Security for Windows Server est installé.

La Console de l'application fait partie des composants d'application "Outils d'administration".

### Utilitaire de la ligne de commande

Vous pouvez administrer Kaspersky Security for Windows Server via la ligne de commande du serveur protégé.

L'utilitaire de ligne de commande fait partie des composants logiciels de Kaspersky Security for Windows Server.

### Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center afin de centraliser l'administration de la protection antivirus des ordinateurs de votre entreprise, vous pourrez administrer Kaspersky Security for Windows Server via la Console d'administration Kaspersky Security Center.

Il faudra installer les composants suivants :

- **Module d'intégration de l'Agent d'administration de Kaspersky Security Center.** Ce composant fait partie des composants logiciels de Kaspersky Security for Windows Server. Il garantit la communication entre Kaspersky Security for Windows Server et l'Agent d'administration. Installez le module d'intégration à l'Agent d'administration Kaspersky Security Center sur le serveur protégé.
- **Agent d'administration Kaspersky Security Center** Installez-le sur chaque serveur protégé. Ce composant garantit l'interaction entre la copie de Kaspersky Security for Windows Server sur le serveur et la Console d'administration Kaspersky Security Center. Le fichier d'installation de l'Agent d'administration fait

partie du kit de distribution de Kaspersky Security Center.

- **Plug-in d'administration de Kaspersky Security 10.1.2.** De plus, sur le serveur où est installé le Serveur d'administration Kaspersky Security Center, installez le plug-in d'administration pour pouvoir utiliser la Console d'administration. Il s'agit de l'interface d'administration de l'application via Kaspersky Security Center. Le fichier d'installation du plug-in d'administration, `\server\klcfiginst.exe`, fait partie du kit de distribution de Kaspersky Security for Windows Server.

## Sélection du type d'installation

Après avoir sélectionné les composants logiciels pour l'installation de Kaspersky Security for Windows Server (cf. section "Codes des composants logiciels de Kaspersky Security for Windows Server pour le service Windows Installer" à la page [36](#)), sélectionnez la méthode d'installation de l'application.

Sélectionnez le mode d'installation en fonction de l'architecture du réseau et des conditions suivantes :

- Que vous ayez besoin de paramètres d'installation spéciaux pour Kaspersky Security for Windows Server ou des paramètres recommandés (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page [44](#)).
- Paramètres d'installation identiques pour tous les serveurs ou propres à chaque serveur ?

Vous pouvez installer Kaspersky Security for Windows Server à l'aide d'un assistant Installation ou en mode silencieux en exécutant le package d'installation selon les paramètres d'installation via la ligne de commande. Vous pouvez réaliser une installation centralisée à distance de Kaspersky Security for Windows Server via les stratégies de groupe Active Directory ou à l'aide d'une tâche d'installation à distance de Kaspersky Security Center.

Vous pouvez installer et configurer Kaspersky Security for Windows Server sur un serveur, en enregistrant ses paramètres dans un fichier de configuration ; le fichier peut être utilisé pour installer Kaspersky Security for Windows Server sur d'autres serveurs (cette possibilité n'est pas offerte en cas d'installation de l'application via des stratégies de groupe Active Directory).

### Lancement de l'Assistant d'installation

Grâce à l'Assistant d'installation, vous pouvez installer :

- les composants de Kaspersky Security for Windows Server (cf. section "Composants de l'application Kaspersky Security for Windows Server" à la page [37](#)) sur un serveur protégé à l'aide du fichier `\server\setup.exe` repris dans le kit de distribution ;
- la console de Kaspersky Security for Windows Server (cf. section "Installation de la console de Kaspersky Security for Windows Server" à la page [53](#)) à l'aide du fichier `\client\setup.exe` du kit de distribution sur le serveur protégé ou sur un autre hôte LAN.

### Lancement du package d'installation via la ligne de commande selon les paramètres d'installation requis

Si vous lancez le fichier du package d'installation sans les options de la ligne de commande, Kaspersky Security for Windows Server sera installé selon les paramètres par défaut. Grâce aux arguments de Kaspersky Security for Windows Server, vous pouvez modifier les paramètres d'installation.

Vous pouvez installer la console de l'application sur le serveur protégé et/ou sur le poste de travail de l'administrateur.

Vous pouvez aussi utiliser des exemples de commande pour l'installation de Kaspersky Security for Windows Server et de la Console de l'application (cf. section "Installation et suppression de l'application via la ligne de commande" à la page [65](#)).

### Installation centralisée via Kaspersky Security Center

Si vous utilisez Kaspersky Security Center dans votre réseau pour administrer la protection antivirus des serveurs en réseau, vous pouvez installer Kaspersky Security for Windows Server sur plusieurs serveurs à l'aide de la tâche d'installation à distance.

Les serveurs sur lesquels vous souhaitez installer Kaspersky Security for Windows Server via Kaspersky Security Center (cf. section "Installation et suppression de l'application via Kaspersky Security Center" à la page [71](#)) peuvent soit se trouver dans le même domaine que Kaspersky Security Center, soit dans un autre domaine. Ils peuvent également n'appartenir à aucun domaine.

### Installation centralisée via les stratégies de groupe Active Directory

Les stratégies de groupe Active Directory permettent d'installer Kaspersky Security for Windows Server sur un serveur protégé. Vous pouvez également installer la console de l'application sur le serveur protégé ou sur le poste de travail de l'administrateur.

Vous pouvez installer Kaspersky Security for Windows Server uniquement avec les paramètres par défaut.

Les serveurs sur lesquels Kaspersky Security for Windows Server est installé à l'aide des stratégies de groupe Active Directory (cf. section "Installation et suppression de l'application à l'aide de stratégies de groupe Active Directory" à la page [76](#)) doivent se trouver dans le même domaine et dans la même unité organisationnelle. L'installation a lieu lors du démarrage du serveur avant la connexion à Microsoft Windows.

## Installation et suppression de l'application à l'aide de l'assistant

La section décrit l'installation et la désinstallation de Kaspersky Security for Windows Server et de la Console de l'application via l'assistant Installation. Elle contient des informations sur la configuration avancée de Kaspersky Security for Windows Server et définit les actions à réaliser lors de l'installation.

### Dans cette section

Installation à l'aide de l'Assistant d'installation .....	<a href="#">50</a>
Modification de la sélection de composants et réparation de Kaspersky Security for Windows Server .....	<a href="#">62</a>
Suppression à l'aide de l'Assistant d'installation .....	<a href="#">63</a>

## Installation à l'aide de l'Assistant d'installation

Les sections suivantes contiennent des informations sur l'installation de Kaspersky Security for Windows Server, de la Console de l'application et du Plug-in pour Microsoft Outlook.

► *Pour installer et utiliser Kaspersky Security for Windows Server, procédez comme suit :*

1. Installez Kaspersky Security for Windows Server sur un serveur protégé.
2. Installez la console de l'application sur les ordinateurs sur lesquels vous avez l'intention d'administrer Kaspersky Security for Windows Server.
3. Si vous avez installé la console de l'application sur n'importe quel ordinateur du réseau autre que le serveur

protégé, procédez à une configuration complémentaire afin que les utilisateurs de la Console de l'application puissent administrer Kaspersky Security for Windows Server à distance.

4. Installez le Plug-in Microsoft Outlook sur l'ordinateur où le client Microsoft Outlook est installé.
5. Réalisez les actions après l'installation de Kaspersky Security for Windows Server.

## Dans cette section

Installation de Kaspersky Security for Windows Server .....	<a href="#">51</a>
Installation de la console de Kaspersky Security for Windows Server .....	<a href="#">53</a>
Installation du Plug-in Kaspersky Security Microsoft Outlook .....	<a href="#">54</a>
Configuration avancée après l'installation de la console de l'application sur un autre ordinateur .....	<a href="#">56</a>
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	<a href="#">59</a>

## Installation de Kaspersky Security for Windows Server

Avant d'installer Kaspersky Security for Windows Server, suivez ces étapes :

- Assurez-vous qu'aucun autre logiciel antivirus n'est installé sur le serveur. Vous devez désinstaller Kaspersky Antivirus 8.0 for Windows Servers Enterprise Edition. Vous pouvez installer Kaspersky Security for Windows Server 10.1.2 sans désinstaller Kaspersky Security 10 for Windows Server ou suivant.
- Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au groupe d'administrateurs du serveur protégé.

Lorsque les actions décrites ci-dessus ont été effectuées, passez à la procédure d'installation. Définissez les paramètres d'installation de Kaspersky Security for Windows Server en suivant les instructions de l'Assistant. Vous pouvez interrompre l'installation de Kaspersky Security for Windows Server à n'importe quelle étape de l'assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'assistant d'installation.

Vous pouvez obtenir de plus amples informations sur les paramètres d'installation (de désinstallation) (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page [44](#)).

### ► *Pour installer Kaspersky Security for Windows Server à l'aide de l'Assistant d'installation :*

1. Lancez le fichier setup.exe sur le serveur.
2. Dans la section **Installation** de la fenêtre qui s'ouvre, cliquez sur le lien **Installer Kaspersky Security for Windows Server**.
3. Dans la fenêtre d'accueil de l'Assistant d'installation de Kaspersky Security for Windows Server, appuyez sur le bouton **Suivant**.  
La fenêtre **Contrat de licence utilisateur final et politique de confidentialité** s'ouvre.
4. Réviser le Contrat de licence et la Politique de confidentialité.
5. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **les termes de ce Contrat de licence utilisateur final** et **Politique de confidentialité décrivant la manipulation des données** afin de poursuivre l'installation.

Si vous n'acceptez pas le Contrat de licence utilisateur final et/ou la Politique de confidentialité, l'installation sera interrompue.

6. Cliquez sur **Suivant**.

Si le serveur dispose d'une version compatible de l'application installée, la fenêtre **Découverte d'une version antérieure de l'application** s'ouvre.

Si aucune version précédente de l'application n'est détectée, passez à l'étape 8 de ces instructions.

7. Pour mettre à niveau la version précédente de l'application, cliquez sur le bouton **Installer**. L'Assistant d'installation mettra à niveau l'application Kaspersky Security for Windows Server 10.1 et enregistrera les paramètres compatibles dans la nouvelle version. Une fois la mise à niveau terminée, l'assistant ouvrira la fenêtre **Installation terminée** (passez à l'Étape 15 de ces instructions).

La fenêtre **Analyse rapide de l'ordinateur avant l'installation** s'ouvre.

8. Dans la fenêtre **Analyse rapide de l'ordinateur avant l'installation**, cochez la case **Rechercher la présence éventuelle de virus sur l'ordinateur** afin de rechercher la présence éventuelle de menaces dans les secteurs d'amorçage des disques locaux du serveur et dans la mémoire système. Cliquez sur **Suivant**. À la fin de l'analyse, les résultats s'affichent dans une fenêtre.

Vous pourrez y consulter les informations relatives aux objets analysés sur le serveur : nombre total d'objets analysés, nombre de menaces découvertes, nombre d'objets infectés et probablement infectés découverts, nombre de processus dangereux ou suspects que Kaspersky Security for Windows Server a supprimés de la mémoire et nombre de processus dangereux ou suspects que l'application n'a pas réussi à supprimer.

Pour voir exactement les fichiers qui ont été analysés, cliquez sur le bouton **Liste des objets traités**.

9. Dans la fenêtre **Analyse rapide de l'ordinateur avant l'installation**, cliquez sur le bouton **Suivant**.

La fenêtre **Installation personnalisée** s'ouvre.

10. Sélectionnez les composants que vous souhaitez installer.

La liste recommandée des composants à installer reprend par défaut tous les composants de Kaspersky Security for Windows Server, à l'exception des composants Gestion du pare-feu et Monitoring des scripts.

Le composant **Prise en charge du protocole SNMP de Kaspersky Security for Windows Server** apparaît dans la liste des composants à installer uniquement si le service **SNMP Microsoft Windows** est installé sur le serveur.

11. Pour annuler toutes les modifications, cliquez sur , cliquez sur le bouton **Réinitialiser** dans la fenêtre **Installation personnalisée**. Cliquez sur **Suivant**.

12. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :

- Le cas échéant, désignez un dossier pour la copie des fichiers de Kaspersky Security for Windows Server.
- Le cas échéant, consultez les informations concernant l'espace disponible sur les disques durs locaux en cliquant sur **Disque**.

Cliquez sur **Suivant**.

13. Dans la fenêtre **Paramètres avancés d'installation** qui s'ouvre, définissez les paramètres d'installation suivants :

- **Activer la protection en temps réel après l'installation de l'application.**

- **Ajouter les exclusions recommandées par Microsoft.**
- **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions.**

Cliquez sur **Suivant**.

14. Dans la fenêtre **Importation des paramètres du fichier de configuration**, procédez comme suit :

- a. Désignez le fichier de configuration pour importer les paramètres de Kaspersky Security for Windows Server depuis un fichier de configuration existant créé dans n'importe quelle version précédente compatible de l'application.
- b. Cliquez sur **Suivant**.

15. Dans la fenêtre **Activation de l'application**, exécutez l'une des actions suivantes :

- Si vous souhaitez activer l'application, sélectionnez un fichier clé de Kaspersky Security for Windows Server.
- Si vous souhaitez activer l'application plus tard, cliquez sur **Suivant**.
- si vous aviez déjà enregistré un fichier clé dans le dossier \server du kit de distribution, le nom de ce fichier apparaît dans le champ **Clé**.
- Si vous souhaitez ajouter une licence à l'aide d'un fichier clé qui se trouve dans un autre dossier, spécifiez le fichier clé.

**Vous ne pouvez pas activer l'application à l'aide d'un code d'activation via l'Assistant d'installation. Si vous souhaitez activer l'application à l'aide d'un code d'activation, vous devez saisir le code après l'installation.**

Après l'ajout du fichier clé, la fenêtre affiche les informations concernant la licence. Kaspersky Security for Windows Server la date d'expiration de la licence calculée. La date de validité de la licence est calculée à partir de l'ajout de la clé et elle ne dépasse jamais la date d'expiration de la validité du fichier clé.

Cliquez sur **Suivant** pour appliquer le fichier clé dans l'application.

16. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**. L'assistant lance l'installation des composants de Kaspersky Security for Windows Server.

17. La fenêtre **Installation terminée** s'ouvre à la fin de l'installation.

18. Cochez la case **Lire les notes de publication** afin de consulter les informations relatives à la version après la fin de l'Assistant d'installation.

19. Cliquez sur **Terminer**.

L'assistant d'installation se ferme. Une fois l'installation terminée, Kaspersky Security for Windows Server est prêt à l'emploi si vous avez ajouté une clé d'activation.

## Installation de la console de Kaspersky Security for Windows Server

Configurez la console de l'application en suivant les instructions de l'Assistant d'installation. Vous pouvez interrompre l'installation à n'importe quelle étape de l'Assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'Assistant d'installation.

► *Pour installer la console de l'application, procédez comme suit :*

1. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au

- groupe des administrateurs sur l'ordinateur.
2. Exécutez le fichier setup.exe sur le serveur.  
La fenêtre de bienvenue de l'application s'ouvre.
  3. Cliquez sur le lien **Installer la console de Kaspersky Security for Windows Server**.  
La fenêtre d'accueil de l'Assistant d'installation s'ouvre.
  4. Cliquez sur **Suivant**.
  5. Relisez les conditions du Contrat de licence utilisateur final dans la fenêtre ouverte, et cochez la case **Je confirme que j'ai lu, compris et que j'accepte l'intégralité des termes de ce Contrat de licence utilisateur final** pour procéder à l'installation.
  6. Cliquez sur **Suivant**.  
La fenêtre **Paramètres avancés d'installation** s'ouvre.
  7. Dans la fenêtre **Paramètres avancés d'installation**, procédez comme suit :
    - Si vous avez l'intention d'administrer Kaspersky Security for Windows Server sur un ordinateur distant à l'aide de la Console de l'application, cochez la case **Autoriser l'accès à distance**.
    - Pour ouvrir la fenêtre **Installation personnalisée** et sélectionner des composants, procédez comme suit :
      - a. Cliquez sur le bouton **Avancé**.  
La fenêtre **Installation personnalisée** s'ouvre.
      - b. Sélectionnez le composant "Outils d'administration" dans la liste.  
Par défaut, tous les composants sont installés.
      - c. Cliquez sur **Suivant**.

Vous pouvez obtenir de plus amples informations sur les composants de Kaspersky Security (cf. Section "Codes des composants logiciels de Kaspersky Security for Windows Server pour le service Windows Installer" à la page [36](#)).

8. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :
  - a. Le cas échéant, désignez un autre dossier pour la conservation des fichiers installés.
  - b. Cliquez sur **Suivant**.
9. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**.  
L'Assistant lance l'installation des composants sélectionnés.
10. Cliquez sur **Terminer**.

L'assistant d'installation se ferme. La Console de l'application sera installée sur le serveur protégé.

Si vous avez installé la sélection Outils d'administration sur tout ordinateur du réseau autre que le serveur protégé, configurez les paramètres avancés (cf. section "Configuration avancée après l'installation de la console de l'application sur un autre ordinateur" à la page [56](#)).

## Installation du Plug-in Kaspersky Security Microsoft Outlook

Suivez les instructions de l'Assistant d'installation pour configurer les paramètres d'installation du Plug-in Microsoft



Outlook. Le processus d'installation peut être interrompu à n'importe quelle étape de l'Assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'Assistant d'installation.

Vous pouvez installer le Plug-in Microsoft Outlook sur le serveur protégé seulement si Kaspersky Security for Windows Server et le client de messagerie Microsoft Outlook sont installés.

► Pour installer le Plug-in Microsoft Outlook, procédez comme suit :

1. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au groupe des administrateurs sur l'ordinateur.
2. Exécutez le fichier setup.exe sur le serveur.  
La fenêtre de bienvenue de l'application s'ouvre.
3. Cliquez sur le lien **Lancez le complément Microsoft Outlook (x86) de Kaspersky Security 10.1** ou **Lancez le complément Microsoft Outlook (x64) de Kaspersky Security 10.1** en fonction du nombre de bits du client Microsoft Outlook installé.  
La fenêtre d'accueil de l'Assistant d'installation s'ouvre.
4. Cliquez sur **Suivant**.
5. Relisez les conditions du Contrat de licence utilisateur final dans la fenêtre ouverte, et cochez la case **Je confirme que j'ai lu, compris et que j'accepte l'intégralité des termes de ce Contrat de licence utilisateur final** pour procéder à l'installation.
6. Cliquez sur **Suivant**.  
La fenêtre **Dossier de destination** s'ouvre.
7. Dans la fenêtre **Dossier de destination** qui s'ouvre :
  - Si vous souhaitez modifier le dossier de destination, cliquez sur le bouton **Modifier**.  
La fenêtre **Modifier le dossier de destination** s'ouvre.
    - a. Indiquez un autre dossier de destination.
    - b. Cliquez sur le bouton **OK**.
  - Si vous ne souhaitez pas modifier le dossier de destination, cliquez sur le bouton **Suivant**.  
La fenêtre **Prêt à installer le Plug-in Kaspersky Security for Windows Server 10.1 pour Microsoft Outlook** s'ouvre.
8. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**.  
L'Assistant lance l'installation des composants sélectionnés.
9. Cliquez sur **Terminer**.  
L'assistant d'installation se ferme.

Si le client de messagerie Microsoft Outlook est en cours d'exécution pendant l'installation du Plug-in, vous devez le redémarrer après la fin de l'installation.

## Configuration avancée après l'installation de la console de l'application sur un autre ordinateur

Si vous avez installé la Console de l'application sur tout ordinateur du réseau autre qu'un serveur protégé, réalisez les actions suivantes afin que les utilisateurs puissent administrer Kaspersky Security for Windows Server à distance :

- Sur le serveur protégé, ajoutez les utilisateurs de Kaspersky Security for Windows Server au groupe KAVWSEE Administrators.
- Autorisez les connexions réseau pour le Service Kaspersky Security Management (kavfsgt.exe) (voir section "A propos des autorisations d'accès au Service Kaspersky Security Management" à la page [243](#)) si le pare-feu Windows ou un pare-feu tiers est utilisé sur le serveur protégé.
- Si lors de l'installation de la Console de l'application sur un ordinateur tournant sous Microsoft Windows vous n'avez pas coché la case **Autoriser l'accès à distance**, autorisez manuellement les connexions réseau pour la Console de l'application via le pare-feu de cet ordinateur.

La Console de l'application sur l'ordinateur distant utilise le protocole DCOM pour obtenir les informations sur les événements de Kaspersky Security for Windows Server (objets analysés, tâches terminées, etc.) fournies par le Service Kaspersky Security Management sur le serveur protégé. Vous devez autoriser les connexions réseau pour la Console de l'application dans le pare-feu Windows pour la Console de l'application afin d'établir une connexion entre la Console de l'application et le Service Kaspersky Security Management.

Sur l'ordinateur distant où la Console de l'application est installée, procédez comme suit :

- 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 réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Security for Windows Server.

L'ordinateur sur lequel la Console de l'application est installée utilise le port TCP 135 pour accéder au serveur protégé et pour recevoir une réponse.

- Configurez une règle sortante pour que le pare-feu Windows autorise la connexion.

Contrairement aux services TCP/IP et UDP/IP classiques où un seul protocole est associé à un port fixe, le service DCOM affecte des ports de manière dynamique aux objets COM distants. Si un pare-feu existe entre le client (ou la Console de l'application est installée) et le terminal DCOM (le serveur protégé), un grand éventail de ports doit être ouvert.

Les mêmes étapes doivent être appliquées pour configurer tout autre pare-feu logiciel ou matériel.

► Si la Console de l'application est ouverte pendant que vous configurez la connexion entre le serveur protégé et l'ordinateur sur lequel elle est installée, procédez comme suit :

1. Fermez la console de l'application.
2. Attendez la fin du processus de gestion à distance de Kaspersky Security for Windows Server kavfsrcn.exe.
3. Redémarrez la console de l'application.

Les nouvelles valeurs des paramètres de connexion seront appliquées.

## Dans cette section

Autorisation de l'accès à distance anonyme aux applications COM .....	57
Autorisation des connexions réseau pour le processus d'administration à distance de Kaspersky Security for Windows Server.....	57
Ajout d'une règle sortante pour le pare-feu Windows.....	58

## Autorisation de l'accès à distance anonyme aux applications COM

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

- *Pour autoriser l'accès à distance anonyme aux applications COM, procédez comme suit :*
  1. Sur l'ordinateur distant sur lequel la console de Kaspersky Security for Windows Server est installée, ouvrez la console du Service des composants.
  2. Choisissez **Démarrer** → **Exécuter**.
  3. Saisissez la commande `dcomcnfg`.
  4. Cliquez sur le bouton **OK**.
  5. Dans la console du **Service des composants** du serveur, développez le nœud **Ordinateurs**.
  6. Ouvrez le menu contextuel du nœud **Poste de travail**.
  7. Choisissez l'option **Propriétés**.
  8. Sous l'onglet **Sécurité COM** de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les limites** du groupe de paramètres **Autorisations d'accès**.
  9. Dans la fenêtre **Autoriser l'accès à distance**, assurez-vous que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur ANONYMOUS LOGON.
  10. Cliquez sur le bouton **OK**.

## Autorisation des connexions réseau pour le processus d'administration à distance de Kaspersky Security for Windows Server

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

- *Pour ouvrir le port TCP 135 du pare-feu Windows et autoriser les connexions de réseau pour le processus d'administration à distance de Kaspersky Security for Windows Server, procédez comme suit :*
  1. Sur l'ordinateur distant, fermez la console de Kaspersky Security for Windows Server.
  2. Exécutez une des actions suivantes :

- Dans Microsoft Windows XP ou Microsoft Windows Vista :
    - a. Dans Microsoft Windows XP Service Pack 2 ou supérieur, sélectionnez **Démarrer > Pare-feu Windows**.  
Dans Microsoft Windows Vista, sélectionnez **Démarrer > Panneau de configuration > Pare-feu Windows** et, dans la fenêtre **Pare-feu Windows**, sélectionnez l'option **Modifier les paramètres**.
    - b. Dans la fenêtre **Pare-feu Windows** (ou Paramètres du pare-feu Windows), cliquez sur le bouton **Ajouter un port** sous l'onglet **Exclusions**.
    - c. Dans le champ **Nom**, indiquez le nom du port RPC (TCP/135) ou saisissez un autre nom, par exemple DCOM Kaspersky Security for Windows Server et dans le champ **Nom de port**, indiquez le numéro du port : 135.
    - d. Sélectionnez le protocole **TCP**.
    - e. Cliquez sur le bouton **OK**.
    - f. Sous l'onglet **Exclusions**, cliquez sur le bouton **Ajouter**.
  - Dans Microsoft Windows 7 et suivants :
    - a. Sélectionnez **Démarrer > Panneau de configuration > Pare-feu Windows**.
    - b. Dans la fenêtre **Pare-feu Windows**, sélectionnez **Autoriser le lancement de l'application ou du module via le Pare-feu Windows**.
    - c. Dans la fenêtre **Autoriser un programme via le Pare-feu Windows**, cliquez sur le bouton **Autoriser un autre programme**.
3. Dans la fenêtre **Ajout de programme**, désignez le fichier kavfsrnc.exe. Il se trouve dans le dossier cible désigné lors de l'installation de la console de Kaspersky Security for Windows Server à l'aide de Microsoft Management Console.
  4. Cliquez sur le bouton **OK**.
  5. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu Windows (Paramètres du pare-feu Windows)**.

## Ajout d'une règle sortante pour le pare-feu Windows

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

► Pour ajouter la règle sortante pour le pare-feu Windows, procédez comme suit :

1. Sélectionnez **Démarrer > Panneau de configuration > Pare-feu Windows**.
2. Dans la fenêtre **Pare-feu Windows**, cliquez sur le lien **Paramètres avancés**.  
La fenêtre **Pare-feu Windows avec sécurité avancée** s'ouvre.
3. Cochez le nœud enfant **Règles de trafic sortant**.
4. Dans le panneau **Actions**, cliquez sur l'option **Nouvelle règle**.
5. Dans la fenêtre de l'**assistant de création de nouvelle règle de sortie**, sélectionnez l'option **Port** et cliquez sur **Suivant**.
6. Sélectionnez le protocole **TCP**.
7. Dans le champ **Ports distants spécifiques**, spécifiez la plage de ports suivante pour autoriser les

connexions sortantes : 1024-65535.

8. Dans la fenêtre **Action**, sélectionnez l'option **Autoriser la connexion**.
9. Enregistrez la nouvelle règle et fermez la fenêtre **Pare-feu Windows avec fonctions avancées de sécurité**.

Le pare-feu Windows autorise désormais les connexions réseau entre la console de l'application et le Service Kaspersky Security Management :

## Actions à réaliser après l'installation de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si l'option **Activer la protection en temps réel après l'installation de l'application** (option par défaut) est sélectionnée lors de l'installation de Kaspersky Security for Windows Server, l'application analyse les objets du système de fichiers du serveur lorsqu'ils sont sollicités. Si le composant Monitoring des scripts a été installé lors de l'installation personnalisée, Kaspersky Security for Windows Server analyse le code de programme de tous les scripts quand ils sont exécutés. Kaspersky Security for Windows Server exécutera la tâche Analyse des zones critiques tous les vendredis à 20h00.

Après l'installation de Kaspersky Security for Windows Server, il est conseillé de réaliser les actions suivantes :

- Lancez la tâche Mise à jour des bases de l'application. Une fois installé, Kaspersky Security for Windows Server analyse les objets à l'aide des bases livrées avec le kit de distribution de l'application.

Nous recommandons de mettre à jour immédiatement les bases de Kaspersky Security for Windows Server car elles peuvent être obsolètes.

Par la suite, l'application mettra à jour les bases toutes les heures conformément à la planification définie dans la tâche par défaut.

- Lancer une analyse rapide du serveur si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur le serveur protégé avant l'installation de Kaspersky Security for Windows Server.
- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security for Windows Server.

### Dans cette section

Lancement et configuration de la tâche de mise à jour des bases de données de Kaspersky Security for Windows Server.....	<a href="#">59</a>
Analyse des zones critiques .....	<a href="#">61</a>

## Lancement et configuration de la tâche de mise à jour des bases de données de Kaspersky Security for Windows Server

► Pour mettre à jour les bases de l'application après l'installation, procédez comme suit :

1. Configurer la connexion avec une source de mise à jour, les serveurs HTTP ou FTP de mise à jour de

Kaspersky Lab, dans les propriétés de la tâche Mise à jour des bases de l'application.

2. Lancer la tâche Mise à jour des bases de l'application.

Le protocole WPAD (Web Proxy Auto-Discovery) n'est peut-être pas configuré sur votre réseau pour détecter automatiquement les paramètres du serveur proxy dans le LAN. De plus, le réseau requiert peut-être l'authentification pour accéder au serveur proxy.

- *Pour définir les paramètres du serveur proxy en option ainsi que les paramètres d'authentification pour accéder au serveur proxy, procédez comme suit :*

1. Ouvrez le menu contextuel du nœud **Kaspersky Security** .
2. Sélectionnez l'option **Propriétés**.  
La fenêtre **Paramètres de l'application** s'ouvre.
3. Ouvrez l'onglet **Paramètres de connexion**.
4. Dans la section **Paramètres du serveur proxy**, cochez la case **Utiliser les paramètres du serveur proxy indiqué**.
5. Saisissez l'adresse du serveur proxy dans le champ **Adresse** et saisissez le numéro de port du serveur proxy dans le champ **Port**.
6. Dans la section **Paramètres d'authentification du serveur proxy**, sélectionnez la méthode d'authentification nécessaire dans la liste déroulante :
  - **Utiliser l'authentification NTLM** si le serveur proxy prend en charge l'analyse intégrée de l'authenticité dans Microsoft Windows (NTLM authentification). Kaspersky Security for Windows Server accède alors au serveur proxy à l'aide du compte utilisateur indiqué dans les paramètres de la tâche (la tâche est exécutée par défaut sous le compte utilisateur **Système local (SYSTEM)**).
  - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** si le serveur prend en charge l'authentification NTLM Microsoft Windows intégrée. Kaspersky Security for Windows Server utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy. Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
  - **Utiliser le nom d'utilisateur et le mot de passe** pour choisir l'authentification traditionnelle (Basic authentification). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
7. Cliquez sur **OK** dans la fenêtre **Paramètres de l'application**.

- *Pour configurer la connexion aux serveurs de mise à jour de Kaspersky Lab dans la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Lancez la Console de l'application d'une des manières suivantes :
  - Ouvrez la console de l'application sur le serveur protégé. Pour cela, cliquez sur **Démarrer > Tous les programmes > Kaspersky Security for Windows Server > Outils d'administration > Console de Kaspersky Security 10.1.2 for Windows Server**.
  - Si vous avez lancé la Console de l'application sur un serveur autre que celui qui est protégé, connectez-vous au serveur protégé :
    - a. Ouvrez le menu contextuel du nœud **Kaspersky Security** dans l'arborescence de la Console de

l'application.

- b. Sélectionnez l'option **Se connecter à un autre ordinateur**.
- c. Dans la fenêtre **Sélection d'ordinateur** qui s'ouvre, choisissez **Autre ordinateur** et saisissez le nom de réseau du serveur protégé dans le champ textuel.

Si le compte utilisateur employé pour se connecter à Microsoft Windows ne possède pas les autorisations d'accès au Service Kaspersky Security Management (cf. section "A propos des autorisations d'accès au Service Kaspersky Security Management" à la page [243](#)), indiquez un compte utilisateur doté de ces autorisations.

La fenêtre Console de l'application s'ouvre.

2. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
3. Sélectionnez le nœud enfant **Mise à jour des bases de l'application**.
4. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.
5. Dans la fenêtre **Paramètres de la tâche** qui s'ouvre, ouvrez l'onglet **Paramètres de connexion**.
6. Sélectionnez **Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky Lab**.
7. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres de connexion à la source de mise à jour dans la tâche Mise à jour des bases de l'application sont sauvegardés.

► *Pour lancer la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Dans le menu contextuel du nœud enfant **Mise à jour des bases de l'application**, sélectionnez l'option **Démarrer**.

La tâche de Mise à jour des bases de l'application démarre.

Une fois la tâche terminée, vous pouvez consulter la date de publication des dernières mises à jour des bases de l'application installées dans le panneau de détails du nœud **Kaspersky Security**.

## Analyse des zones critiques

Une fois que les bases de Kaspersky Security for Windows Server ont été mises à jour, recherchez la présence éventuelle d'applications malveillantes sur le serveur à l'aide de la tâche Analyse des zones critiques.

► *Pour lancer la tâche Analyse des zones critiques, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Dans le menu contextuel du nœud enfant **Analyse des zones critiques**, sélectionnez la commande **Démarrer**.

La tâche est lancée et l'état **Exécution en cours** apparaît dans le volet des détails.

► *Pour consulter le journal d'exécution de la tâche,*

dans le panneau de détails du nœud **Analyse des zones critiques**, cliquez sur le lien **Ouvrir le journal**



d'exécution de la tâche.

## Modification de la sélection de composants et réparation de Kaspersky Security for Windows Server

Vous pouvez ajouter ou supprimer des composants de Kaspersky Security for Windows Server. Vous devez d'abord arrêter la tâche Protection des fichiers en temps réel si vous souhaitez supprimer le composant Protection des fichiers en temps réel. Dans tous les autres cas, il n'est pas nécessaire d'arrêter la Protection des fichiers en temps réel ou le Service Kaspersky Security.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Security for Windows Server requiert la saisie du mot de passe lors de toute tentative de suppression de composants ou de modification de la liste des composants de l'application dans l'assistant d'installation.

► Pour modifier la sélection de composants de Kaspersky Security for Windows Server :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes > Kaspersky Security for Windows Server > Modification ou suppression de Kaspersky Security for Windows Server**.

La fenêtre **Modification, réparation ou suppression** de l'Assistant d'installation s'ouvre.

2. Sélectionnez **Modification de la liste des composants**. Cliquez sur **Suivant**.

La fenêtre **Installation personnalisée** s'ouvre.

3. Dans la liste des composants disponibles qui apparaît dans la fenêtre **Installation personnalisée**, sélectionnez les composants à ajouter ou à supprimer dans Kaspersky Security for Windows Server. Pour ce faire, procédez comme suit :

- Pour modifier la composition des composants, cliquez sur le bouton situé en regard du composant sélectionné. Puis, sélectionnez dans le menu contextuel :
  - L'option **Le composant sera installé sur un disque dur local** si vous souhaitez installer un composant ;
  - L'option **Le composant et ses sous-composants seront installés sur le disque dur local** si vous souhaitez installer un groupe de composants.
- Pour supprimer un composant déjà installé, cliquez sur le bouton en regard du nom du composant sélectionné. Puis sélectionnez **Ce composant ne sera plus disponible** dans le menu contextuel.

Cliquez sur **Suivant**.

4. Dans la fenêtre **Prêt pour l'installation**, confirmez la modification de la liste des composants de l'application en cliquant sur le bouton **Installer**.

5. Dans la fenêtre qui s'ouvre lorsque l'installation est terminée, cliquez sur le bouton **OK**.

La liste des composants de Kaspersky Security for Windows Server sera modifiée conformément aux paramètres définis.

Si des problèmes se présentent durant l'utilisation de Kaspersky Security for Windows Server (Kaspersky Security for Windows Server s'arrête, les tâches se soldent par un échec ou ne sont pas lancées), vous pouvez tenter de réparer Kaspersky Security for Windows Server. Vous pouvez procéder à la réparation en conservant les valeurs actuelles des paramètres de Kaspersky Security for Windows Server ou en sélectionnant le mode qui rétablira

toutes les valeurs par défaut des paramètres de Kaspersky Security for Windows Server.

► *Pour réparer Kaspersky Security for Windows Server après une erreur de l'application ou d'une tâche, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.
2. Sélectionnez **Kaspersky Security for Windows Server**.
3. Sélectionnez **Modification ou suppression de Kaspersky Security for Windows Server**.  
La fenêtre **Modification, réparation ou suppression** de l'Assistant d'installation s'ouvre.
4. Sélectionnez **Réparation des composants installés**. Cliquez sur **Suivant**.  
La fenêtre **Réparation des composants installés** s'ouvre.
5. Dans la fenêtre **Réparation des composants installés**, cochez la case **Rétablir les paramètres recommandés de l'application** si vous souhaitez réinitialiser les paramètres et restaurer les paramètres par défaut de Kaspersky Security for Windows Server. Cliquez sur **Suivant**.
6. Dans la fenêtre **Prêt pour la réparation**, confirmez la réparation de l'application en cliquant sur le bouton **Installer**.
7. Dans la fenêtre qui s'ouvre lorsque la réparation est terminée, cliquez sur le bouton **OK**.  
Kaspersky Security for Windows Server sera réparés conformément aux paramètres définis.

## Suppression à l'aide de l'Assistant d'installation

Cette section contient des instructions pour supprimer Kaspersky Security for Windows Server, la Console de l'application et le Plug-in Microsoft Outlook sur un serveur protégé à l'aide de l'Assistant d'installation/de désinstallation.

### Dans cette section

Désinstallation de Kaspersky Security for Windows Server .....	<a href="#">63</a>
Désinstallation de la Console de Kaspersky Security for Windows Server .....	<a href="#">64</a>
Désinstallation du Plug-in Kaspersky Security pour Microsoft Outlook .....	<a href="#">65</a>

## Désinstallation de Kaspersky Security for Windows Server

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Vous pouvez désinstaller Kaspersky Security for Windows Server du serveur protégé à l'aide de l'Assistant d'installation/de désinstallation.

Il faudra peut-être redémarrer le serveur protégé sur lequel Kaspersky Security for Windows Server a été désinstallé. Le redémarrage peut être reporté.

La suppression, la réparation et l'installation d'une application via le panneau d'administration Windows sont impossibles si le système d'exploitation utilise la fonction Contrôle des comptes utilisateurs (User Account Control) ou si l'accès à l'application est protégé par un mot de passe.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Security for Windows Server requiert la saisie du mot de passe lors de toute tentative de suppression de composants ou de modification de la liste des composants de l'application dans l'assistant d'installation.

► *Pour désinstaller Kaspersky Security for Windows Server :*

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.
2. Sélectionnez **Kaspersky Security for Windows Server**.
3. Sélectionnez **Modification ou suppression de Kaspersky Security for Windows Server**.  
La fenêtre **Modification, réparation ou suppression** de l'Assistant d'installation s'ouvre.
4. Sélectionnez **Suppression des composants de l'application**. Cliquez sur **Suivant**.  
La fenêtre **Paramètres avancés de désinstallation de l'application** s'ouvre.
5. Si nécessaire, dans la fenêtre **Paramètres avancés de désinstallation de l'application**, procédez comme suit :
  - a. Cochez la case **Exporter les objets de la quarantaine** pour que Kaspersky Security for Windows Server exporte les objets qui ont été mis en quarantaine. Cette case est décochée par défaut.
  - b. Cochez la case **Exporter les objets de la sauvegarde** pour exporter les objets de la Sauvegarde de Kaspersky Security for Windows Server. Cette case est décochée par défaut.
  - c. Cliquez sur le bouton **Enregistrer dans** et indiquez le dossier vers lequel vous souhaitez exporter les objets. Par défaut, les objets sont exportés vers le dossier %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\Uninstall.  
Cliquez sur **Suivant**.
6. Dans la fenêtre **Prêt pour la désinstallation**, confirmez l'opération de désinstallation en cliquant sur **Désinstaller**.
7. Dans la fenêtre qui s'ouvre lorsque la désinstallation est terminée, cliquez sur le bouton **OK**.  
Kaspersky Security for Windows Server est désinstallé du serveur protégé.

## Désinstallation de la console de Kaspersky Security for Windows Server

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Vous pouvez désinstaller la console de l'application sur l'ordinateur à l'aide de l'Assistant d'installation/de désinstallation.

Il n'est pas nécessaire de redémarrer le serveur après la désinstallation de la Console de l'application.

► *Pour désinstaller la console de l'application, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.
2. Sélectionnez **Kaspersky Security for Windows Server**.
3. Sélectionnez **Modification ou suppression des Outils d'administration de Kaspersky Security 10.1.2 for Windows Server**.

La fenêtre **Modification, réparation ou suppression** de l'Assistant s'ouvre.

4. Choisissez l'option **Suppression des composants de l'application**, puis cliquez sur **Suivant**.
5. La fenêtre **Prêt pour la désinstallation** s'ouvre. Cliquez sur le bouton **Désinstaller**.  
La fenêtre **Désinstallation terminée** s'ouvre.
6. Cliquez sur le bouton **OK**.

L'opération de désinstallation est terminée et la fenêtre de l'Assistant se ferme.

## Désinstallation du Plug-in Kaspersky Security pour Microsoft Outlook

► *Pour désinstaller le Plug-in Microsoft Outlook :*

1. Exécutez le fichier setup.exe sur le serveur.  
La fenêtre d'accueil de l'Assistant d'installation s'ouvre.
2. Cliquez sur **Suivant**.  
La fenêtre **Réparer ou supprimer l'installation** s'ouvre.
3. Cliquez sur le bouton **Supprimer**.  
La fenêtre **Prêt à installer le Plug-in Kaspersky Security for Windows Server pour Microsoft Outlook** s'ouvre.
4. Cliquez sur le bouton **Supprimer**.  
L'Assistant commence à désinstaller le Plug-in Microsoft Outlook.
5. Cliquez sur **Terminer**.

L'opération de désinstallation est terminée et la fenêtre de l'Assistant se ferme.

## Installation et suppression de l'application via la ligne de commande

Cette section décrit les particularités de l'installation et de la désinstallation de Kaspersky Security for Windows Server via la ligne de commande. Elle fournit également des exemples de commande pour l'installation et la désinstallation de Kaspersky Security for Windows Server et des exemples de commandes pour l'ajout et la suppression de composants de Kaspersky Security for Windows Server via la ligne de commande.

## Dans cette section

A propos de l'installation et de la désinstallation de Kaspersky Security for Windows Server via la ligne de commande .....	<a href="#">66</a>
Exemple de commandes pour l'installation de Kaspersky Security for Windows Server.....	<a href="#">66</a>
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	<a href="#">68</a>
Ajout et suppression de composants.Exemples de commandes .....	<a href="#">69</a>
Désinstallation de Kaspersky Security for Windows Server.Exemples de commandes .....	<a href="#">69</a>
Codes de retour .....	<a href="#">70</a>

## A propos de l'installation et de la désinstallation de Kaspersky Security for Windows Server via la ligne de commande

Vous pouvez installer et désinstaller Kaspersky Security for Windows Server, ajouter ou supprimer des composants en exécutant les fichiers du package d'installation `\server\ks4ws_x86(x64).msi` via la ligne de commande et en précisant les paramètres d'installation à l'aide d'arguments.

Vous pouvez installer la sélection "Outils d'administration" sur le serveur protégé ou sur un autre ordinateur du réseau afin d'utiliser la console de l'application localement ou à distance. Pour ce faire, utilisez le paquet d'installation `\client\ks4wstools.msi`.

Réalisez l'installation sous un compte utilisateur appartenant au groupe d'administrateurs du serveur sur lequel l'application est installée.

Si vous exécutez l'un des fichiers `\product\ks4ws_x86(x64).msi` sur le serveur protégé sans clés additionnelles, Kaspersky Security for Windows Server est installé avec les paramètres d'installation recommandés.

Vous pouvez définir la sélection des composants à installer à l'aide de l'argument `ADDLOCAL` en utilisant en guise de valeur le code des composants sélectionnés ou de la sélection de composants.

## Exemple de commandes pour l'installation de Kaspersky Security for Windows Server

Cette section présente des exemples de commandes pour l'installation de Kaspersky Security for Windows Server.

Sur les serveurs fonctionnant sous Microsoft Windows 32 bits, exécutez les fichiers du kit de distribution dont le suffixe est `x86`. Sur les serveurs fonctionnant sous Microsoft Windows 64 bits, exécutez les fichiers du kit de distribution dont le suffixe est `x64`.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des instructions et des clés standard de Windows Installer.

## Exemples d'installation de Kaspersky Security for Windows Server depuis le fichier setup.exe

- Pour installer Kaspersky Security for Windows Server avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande suivante :

```
\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

- Pour installer Kaspersky Security for Windows Server avec les paramètres suivants :

- Installer uniquement les composants Protection des fichiers en temps réel et Analyse à la demande ;
- Ne pas lancer la Protection en temps réel au démarrage de Kaspersky Security for Windows Server ;
- ne pas exclure de la zone d'analyse les fichiers recommandés par Microsoft Corporation ;

saisissez l'instruction suivante :

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

## Exemples de commandes pour l'installation : exécution d'un fichier .msi

- Pour installer Kaspersky Security for Windows Server avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande suivante :

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

- Pour installer Kaspersky Security for Windows Server selon les paramètres recommandés et afficher l'interface d'installation, saisissez la commande suivante :

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

- Pour installer et activer Kaspersky Security for Windows Server à l'aide du fichier clé C:\0000000A.key :

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1  
PRIVACYPOLICY=1
```

- Pour installer Kaspersky Security for Windows Server avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux, saisissez la commande suivante :

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- Pour installer Kaspersky Security for Windows Server dans le dossier d'installation C:\WSEE, exécutez la commande suivante :

```
msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1
```

- Pour installer Kaspersky Security for Windows Server et enregistrer un fichier journal d'installation sous le nom ks4ws.log dans le dossier qui contient le fichier msi de Kaspersky Security for Windows Server, exécutez la commande suivante :

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

- Pour installer la console de Kaspersky Security for Windows Server, exécutez la commande suivante :

```
msiexec /i ks4wstools.msi /qn EULA=1
```

- Pour installer le Plug-in Microsoft Outlook pour le client de messagerie Microsoft Outlook 64 bits, exécutez la commande suivante :

```
msiexec /i ksmail_x64.msi /qn EULA=1
```

- Pour installer le Plug-in Microsoft Outlook pour le client de messagerie Microsoft Outlook 32 bits, exécutez la commande suivante :

```
msiexec /i ksmail_x86.msi /qn EULA=1
```

- Pour installer et activer Kaspersky Security for Windows Server à l'aide du fichier clé C:\0000000A.key et configurer Kaspersky Security for Windows Server conformément aux paramètres du fichier de configuration C:\settings.xml, saisissez la commande suivante :

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key  
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- Pour installer un correctif de l'application lorsque Kaspersky Security for Windows Server est protégé par mot de passe, exécutez la commande suivante :

```
msiexec /p "<nom de fichier msp avec le chemin>" UNLOCK_PASSWORD=<mot de  
passe>
```

## Actions à réaliser après l'installation de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si vous sélectionnez **Activer la protection en temps réel après l'installation de l'application** pendant l'installation de Kaspersky Security for Windows Server, l'application analyse les objets du système de fichiers du serveur au moment d'y accéder. Si le composant Monitoring des script a été installé lors de l'installation personnalisée, Kaspersky Security for Windows Server analyse le code de programme de tous les scripts lorsqu'ils sont exécutés. Chaque vendredi à 20h00, Kaspersky Security for Windows Server lance la tâche Analyse des zones critiques.

Après l'installation de Kaspersky Security for Windows Server, il est conseillé de réaliser les actions suivantes :

- Lancer la tâche de mise à jour des bases de l'application de Kaspersky Security for Windows Server. Une fois installé, Kaspersky Security for Windows Server analyse les objets à l'aide des bases livrées avec le kit de distribution. Nous conseillons de réaliser une mise à jour immédiate des bases de Kaspersky Security for Windows Server. Pour ce faire, vous devez lancer la tâche Mise à jour des bases de l'application. Par la suite, la mise à jour des bases de données sera exécutée toutes les heures selon la planification définie par défaut.

Par exemple, vous pouvez lancer la tâche Mise à jour des bases de l'application à l'aide de l'instruction suivante :

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser  
/PROXYPWD:123456 :
```



Dans ce cas, les mises à jour des bases de données de Kaspersky Security for Windows Server sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab. La connexion à une source de mise à jour est établie via un serveur proxy (adresse du serveur proxy : proxy.company.com, port : 8080) à l'aide de l'authentification Windows NTLM pour accéder au serveur sous un compte (nom d'utilisateur : inetuser ; mot de passe : 123456).

- Lancer une analyse rapide du serveur si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur le serveur protégé avant l'installation de Kaspersky Security for Windows Server.
- *Pour réaliser la tâche Analyse des zones critiques à l'aide d'une ligne de commande, exécutez la commande suivante :*

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Cette instruction conserve le journal d'exécution de la tâche dans le fichier scancritical.log du dossier actif.

- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security for Windows Server.

## Ajout et suppression de composants. Exemples de commandes

Le composant "Analyse à la demande" est installé automatiquement. Il n'est pas nécessaire de l'indiquer dans la liste des valeurs de la clé ADDLOCAL lors de la suppression ou de l'ajout de composants de Kaspersky Security for Windows Server.

- *Pour ajouter le composant Contrôle du lancement des applications aux composants déjà installés, exécutez la commande suivante :*

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn
```

ou

```
\server\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Si vous dressez la liste non seulement des composants que voulez installer, mais également de ceux qui sont déjà installés, Kaspersky Security for Windows Server installe à nouveau les composants indiqués installés.

- *Pour supprimer les composants installés, exécutez la commande suivante :*

```
msiexec /i ks4ws.msi  
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspector,  
AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram  
Disk REMOVE=AppCtrl,Fim" /qn
```

## Désinstallation de Kaspersky Security for Windows Server. Exemples de commandes

- *Pour désinstaller Kaspersky Security for Windows Server sur le serveur protégé, saisissez la*

commande suivante :

```
msiexec /x ks4ws.msi /qn
```

ou

- Sous un système d'exploitation 32 bits :

```
msiexec /x {6607EF9A-4D10-4D3E-B255-6F280BFB3791} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843} /qn
```

- Pour désinstaller la console de Kaspersky Security for Windows Server, saisissez la commande suivante :

```
msiexec /x ks4wstools.msi /qn
```

ou

- Sous un système d'exploitation 32 bits :

```
msiexec /x {54B7D218-5645-46DD-8660-41B336E1BD8A} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {C10F9B07-7FC9-43C0-A5DC-B6CE8A817D76} /qn
```

- Pour désinstaller Kaspersky Security for Windows Server d'un serveur protégé sur lequel la protection par mot de passe est activée, saisissez la commande suivante :

- Sous un système d'exploitation 32 bits :

```
msiexec /x {6607EF9A-4D10-4D3E-B255-6F280BFB3791} UNLOCK_PASSWORD=*** /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {93EDBC7E-D73F-4401-84A5-79E8CBB8B843} UNLOCK_PASSWORD=*** /qn
```

- Pour désinstaller le Plug-in Microsoft Outlook, procédez comme suit :

- Sous un système d'exploitation 32 bits :

```
msiexec /x {6AF88E70-817E-4FFE-8389-04A345E7A3D6} /qn
```

- Sous un système d'exploitation 64 bits :

```
msiexec /x {410BC997-5B96-41B3-8B31-AAA074FE728B} /qn
```

## Codes de retour

Le tableau ci-dessous décrit les codes de retour de la ligne de commande.

Tableau 6. Codes de retour

Code	Description
1324	Le nom du dossier d'installation contient des caractères interdits.

Code	Description
25001	Privilèges insuffisants pour installer Kaspersky Security for Windows Server. Afin d'installer l'application, lancez l'Assistant d'installation avec les privilèges d'administrateur local.
25003	Impossible d'installer Kaspersky Security for Windows Server sur des ordinateurs tournant sous cette version de Microsoft Windows. Veuillez lancer l'Assistant d'installation de l'application prévu pour la version 64 bits de Microsoft Windows.
25004	Une application incompatible a été détectée. Pour continuer l'installation, désinstallez les logiciels suivants : <liste des logiciels incompatibles>.
25010	Le chemin d'accès indiqué ne peut être utilisé pour conserver des objets en quarantaine.
25011	Le nom du dossier de conservation des objets en quarantaine contient des caractères interdits.
26251	Echec du chargement de la DLL pour les Compteurs de performance.
26252	Echec du chargement de la DLL pour les Compteurs de performance.
27300	Impossible d'installer le pilote.
27301	Impossible de supprimer le pilote.
27302	Impossible d'installer le composant réseau. Le seuil maximum d'appareils de filtrage pris en charge a été atteint.
27303	Les bases antivirus sont introuvables.

## Installation et suppression de l'application via Kaspersky Security Center

Cette section contient des informations générales sur l'installation de Kaspersky Security for Windows Server via Kaspersky Security Center. Elle décrit également la procédure d'installation et de désinstallation de Kaspersky Security for Windows Server via Kaspersky Security Center et les actions à réaliser après l'installation de Kaspersky Security for Windows Server.

### Dans cette section

Informations générales sur l'installation via Kaspersky Security Center .....	<a href="#">72</a>
Privilèges pour l'installation ou la désinstallation de Kaspersky Security for Windows Server .....	<a href="#">72</a>
Installation de Kaspersky Security for Windows Server via Kaspersky Security Center.....	<a href="#">73</a>
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	<a href="#">74</a>
Installation de la Console de l'application via Kaspersky Security Center .....	<a href="#">75</a>
Désinstallation de Kaspersky Security for Windows Server via Kaspersky Security Center .....	<a href="#">76</a>

## Informations générales sur l'installation via Kaspersky Security Center

Vous pouvez installer Kaspersky Security for Windows Server via Kaspersky Security Center à l'aide d'une tâche d'installation à distance.

Une fois que cette tâche a été exécutée, Kaspersky Security for Windows Server est installé selon les mêmes paramètres sur plusieurs serveurs.

Vous pouvez rassembler les serveurs dans un seul groupe d'administration et créer une tâche de groupe pour l'installation de Kaspersky Security for Windows Server sur les serveurs de ce groupe.

Vous pouvez créer une tâche d'installation à distance de Kaspersky Security for Windows Server pour une sélection de serveurs qui n'appartiennent pas à un groupe d'administration. Lors de la création de cette tâche, vous devez constituer la liste des serveurs distincts sur lesquels il faut installer Kaspersky Security for Windows Server.

Le *Système d'aide de Kaspersky Security Center* contient des informations supplémentaires sur la tâche d'installation à distance.

## Privilèges pour l'installation ou la désinstallation de Kaspersky Security for Windows Server

Le compte utilisateur que vous spécifiez dans la tâche d'installation (de suppression) à distance doit appartenir au groupe d'administrateurs sur chacun des serveurs protégés dans tous les cas, sauf dans les situations suivantes :

- Les serveurs sur lesquels vous souhaitez installer Kaspersky Security for Windows Server sont déjà dotés de l'Agent d'administration Kaspersky Security Center (quel que soit le domaine où se trouvent les serveurs ou leur appartenance à un domaine quelconque).

Si l'Agent d'administration n'est pas encore installé sur les serveurs, vous pouvez l'installer en même temps que Kaspersky Security for Windows Server à l'aide d'une tâche d'installation à distance. Avant d'installer l'Agent d'administration, assurez-vous que le compte utilisateur indiqué dans la tâche appartient au groupe d'administrateurs sur chacun des serveurs.

- Tous les serveurs sur lesquels vous souhaitez installer Kaspersky Security for Windows Server se trouvent dans le même domaine que le Serveur d'administration et celui-ci est enregistré sous le compte Administrateur de domaine (**Domain Admin**) (si le compte jouit des privilèges d'administrateur local sur les serveurs du domaine).

Par défaut, la tâche d'installation à distance selon la méthode **Installation forcée** s'exécute sous le compte sous les privilèges duquel le Serveur d'administration fonctionne.

Dans les tâches de groupe, ainsi que dans les tâches pour une sélection d'ordinateurs, en mode d'installation (désinstallation) forcée, le compte utilisateur doit posséder les autorisations suivantes sur l'ordinateur client :

- autorisation pour l'exécution à distance des applications ;
- autorisations sur le partage **Admin\$** ;
- autorisation pour **Se connecter en tant que service**.

## Installation de Kaspersky Security for Windows Server via Kaspersky Security Center

Le Manuel d'implantation de Kaspersky Security Center contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

Si vous comptez administrer plus tard Kaspersky Security for Windows Server via Kaspersky Security Center, assurez-vous que les conditions suivantes sont remplies :

- Le plug-in d'administration (fichier \server\klcfginst.exe du kit de distribution de Kaspersky Security for Windows Server) est également installé sur le serveur sur lequel est installé le Serveur d'administration de Kaspersky Security Center.
- Sur les serveurs protégés, l'Agent d'administration de Kaspersky Security Center est installé. Si les serveurs protégés ne sont pas dotés de l'Agent d'administration de Kaspersky Security Center, vous pouvez l'installer en même temps que Kaspersky Security for Windows Server via une tâche d'installation à distance.

Vous pouvez également réunir au préalable les serveurs dans un groupe d'administration afin de pouvoir ultérieurement administrer les paramètres de la protection à l'aide de stratégies ou des tâches de groupe de Kaspersky Security Center.

► *Pour installer Kaspersky Security for Windows Server à l'aide d'une tâche d'installation à distance :*

1. Lancement de la console d'administration de Kaspersky Security Center
2. Dans Kaspersky Security Center, développez le nœud **Avancé**.
3. Développez le nœud enfant **Installation à distance**.
4. Dans le panneau de détails du nœud enfant **Paquets d'installation**, cliquez sur le bouton **Créer un paquet d'installation**.
5. En guise de type de paquet d'installation, sélectionnez l'option **Créer un paquet d'installation pour une application de Kaspersky Lab**.
6. Entrez le nom du paquet d'installation.
7. Spécifiez le fichier ks4ws.kud à partir du kit de distribution de Kaspersky Security for Windows Server comme fichier du paquet d'installation.

La fenêtre **Contrat de licence utilisateur final et Politique de confidentialité** s'ouvre.

8. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **les termes de ce Contrat de licence utilisateur final** et **Politique de confidentialité décrivant la manipulation des données** afin de poursuivre l'installation.

Vous devez accepter le Contrat de licence et la Politique de confidentialité.

9. Pour modifier la sélection des composants de Kaspersky Security for Windows Server à installer (cf. section "Modification de la sélection de composants et réparation de Kaspersky Security for Windows Server" à la page [62](#)) et les paramètres d'installation par défaut (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page [44](#)) dans le paquet d'installation :
  - a. Dans Kaspersky Security Center, développez le nœud **Installation à distance**.
  - b. Dans le panneau de détails du nœud enfant **Paquets d'installation**, ouvrez le menu contextuel du

paquet d'installation créé pour Kaspersky Security for Windows Server et choisissez l'option **Propriétés**.

- c. Dans la fenêtre **Propriétés : <nom du paquet d'installation>**, accédez à la section **Configuration** et réalisez les opérations suivantes :
  - a. Dans le groupe de paramètres **Composants installés**, cochez les cases en regard des noms des composants de Kaspersky Security for Windows Server que vous souhaitez installer.
  - b. Pour désigner un dossier de destination différent du dossier sélectionné par défaut, indiquez le nom du dossier et son chemin d'accès dans le champ **Dossier de destination**.  
Le chemin d'accès au répertoire cible peut contenir des variables système. Si le répertoire indiqué n'existe pas sur le serveur, il sera créé.
  - c. Dans le groupe **Paramètres avancés d'installation**, définissez les valeurs suivantes :
    - Réaliser l'analyse antivirus sur le serveur avant l'installation.
    - Activer la protection en temps réel après l'installation de l'application.
    - Ajouter les exclusions recommandées par Microsoft.
    - Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions.
  - d. Si vous souhaitez importer les paramètres du fichier de configuration créé dans la version précédente de Kaspersky Anti-Virus for Windows Server, indiquez le fichier de configuration requis.
- d. Dans la fenêtre **Propriétés : <nom du paquet d'installation>**, cliquez sur le bouton **OK**.

10. Dans le nœud **Paquets d'installation**, créez une tâche pour installer à distance Kaspersky Security for Windows Server sur les serveurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

L'*Aide de Kaspersky Security Center* contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.

11. Lancez la tâche d'installation à distance de Kaspersky Security for Windows Server.

Kaspersky Security for Windows Server est installé sur les serveurs indiqués dans la tâche.

## Actions à réaliser après l'installation de Kaspersky Security for Windows Server

Après l'installation de Kaspersky Security for Windows Server, il est conseillé de mettre à jour les bases de Kaspersky Security for Windows Server sur les serveurs et de lancer l'analyse rapide des serveurs si ceux-ci n'étaient pas dotés d'un logiciel antivirus avec Protection en temps réel active avant l'installation de Kaspersky Security for Windows Server.

Si les serveurs sur lesquels vous avez installé Kaspersky Security for Windows Server sont réunis dans le même groupe d'administration dans Kaspersky Security Center, vous pouvez exécuter ces tâches de la manière suivante :

1. Créez une tâche de mise à jour des bases de l'application pour le groupe de serveurs sur lesquels vous avez installé Kaspersky Security for Windows Server. Désignez le Serveur d'administration Kaspersky Security Center comme source des mises à jour.
2. Créez une tâche de groupe d'analyse à la demande avec l'état Analyse des zones critiques. Kaspersky Security Center évaluera l'état de la protection de chaque ordinateur du groupe sur la base des résultats de cette tâche et non pas sur la base des résultats de l'Analyse des zones critiques.
3. Créez une stratégie pour le groupe de serveurs. Dans la section **Paramètres de l'application** des

propriétés de la stratégie, désactivez le lancement programmé des tâches d'analyse à la demande système ainsi que des tâches de Mise à jour des bases de l'application sur les serveurs du groupe d'administration dans la sous-section **Lancer les tâches système**.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Security for Windows Server.

## Installation de la console de l'application via Kaspersky Security Center

Le Manuel d'implantation de Kaspersky Security Center contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

► Pour installer la console de l'application à l'aide d'une tâche d'installation à distance, procédez comme suit :

1. Dans la Console d'administration de Kaspersky Security Center, développez le nœud **Avancé**.
2. Développez le nœud enfant **Installation à distance**.
3. Dans le panneau de détails du nœud enfant Paquets d'installation, cliquez sur le bouton **Créer un paquet d'installation**. Création d'un paquet d'installation :
  - a. Dans la fenêtre **Assistant Nouveau paquet d'installation**, sélectionnez **Créer** un paquet d'installation pour le fichier exécutable défini en tant que type de paquet.
  - b. Saisissez le nom du nouveau paquet d'installation.
  - c. Sélectionnez le fichier client\setup.exe dans le dossier du kit de distribution de Kaspersky Security for Windows Server, puis cochez la case **Copier tout le dossier dans le paquet d'installation**.
  - d. Le cas échéant, modifiez la liste des composants à installer dans le champ **Paramètres de lancement du fichier exécutable (facultatif)** à l'aide de l'argument ADDLOCAL et modifiez le dossier cible.

Par exemple, pour installer la Console de l'application seule dans le dossier C:\KasperskyConsole sans le fichier d'aide et la documentation, utilisez les options de ligne de commande suivantes :

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
```

4. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la Console de l'application sur les serveurs sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

L'Aide de Kaspersky Security Center contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.

5. Lancez la tâche d'installation à distance.

La console de l'application est installée sur les ordinateurs désignés dans la tâche.



## Désinstallation de Kaspersky Security for Windows Server via Kaspersky Security Center

Si l'administration de Kaspersky Security for Windows Server sur les ordinateurs du réseau est protégée par mot de passe, il faut saisir le mot de passe au moment de la création d'une tâche de désinstallation de plusieurs applications. Si la protection par mot de passe n'est pas gérée centralement par une stratégie de Kaspersky Security Center, Kaspersky Security for Windows Server est supprimé sur les serveurs si le mot de passe saisi correspond à la valeur définie. Kaspersky Security for Windows Server n'est pas désinstallé sur les autres ordinateurs.

► Pour supprimer Kaspersky Security for Windows Server, procédez comme suit dans la Console d'administration de Kaspersky Security Center :

1. Dans la Console d'administration Kaspersky Security Center, créez et lancez une tâche de suppression de l'application.
2. Dans la tâche, sélectionnez la méthode de désinstallation (comme vous aviez choisi la méthode d'installation, cf. section précédente) et désignez le compte sous lequel le Serveur d'administration accédera aux serveurs. Vous pouvez désinstaller Kaspersky Security for Windows Server uniquement selon les paramètres de désinstallation par défaut (cf. section "Paramètres d'installation et de suppression et arguments correspondant pour le service Windows Installer" à la page [44](#)).

## Installation et suppression via les stratégies de groupe Active Directory

Cette section décrit l'installation et la désinstallation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory. Elle fournit également des informations sur les actions requises après l'installation de Kaspersky Security for Windows Server via des stratégies de groupe.

### Dans cette section

Installation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory .....	<a href="#">76</a>
Actions à réaliser après l'installation de Kaspersky Security for Windows Server .....	<a href="#">77</a>
Désinstallation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory .....	<a href="#">78</a>

## Installation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory

Vous pouvez installer Kaspersky Security for Windows Server sur plusieurs serveurs à l'aide d'une stratégie de groupe Active Directory. Vous pouvez, de la même manière, installer la console de l'application.

Les serveurs sur lesquels vous souhaitez installer Kaspersky Security for Windows Server ou la Console de

l'application doivent appartenir au même domaine et à une seule unité d'organisation.

Les systèmes d'exploitation des serveurs sur lesquels vous souhaitez installer Kaspersky Security for Windows Server à l'aide de la stratégie doivent tous avoir le même nombre de bits (32 ou 64 bits).

Vous devez posséder les autorisations d'administrateur de domaine.

Pour installer Kaspersky Security for Windows Server, utilisez les paquets d'installation ks4ws\_x86(x64).msi. Pour installer la console de l'application, utilisez le paquet d'installation ks4wstools.msi.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

► Pour installer Kaspersky Security for Windows Server (ou la console de l'application) :

1. Enregistrez le fichier msi du paquet d'installation de la version correspondante du système d'exploitation de Microsoft Windows (32 ou 64 bits) dans un dossier partagé sur le contrôleur de domaine.
2. Enregistrez le fichier clé (cf. section "A propos du fichier clé" sur la page [85](#)) dans le même dossier public sur le contrôleur de domaine.
3. Dans ce dossier partagé sur le contrôleur de domaine, créez un fichier install\_props.json contenant les éléments ci-après afin de confirmer que vous acceptez les dispositions du Contrat de licence et de la Politique de confidentialité.

```
{
  "EULA" : "1",
  "PRIVACYPOLICY" : "1"
}
```

4. Sur le contrôleur de domaine, créez une stratégie pour groupe auquel appartiennent les serveurs.
5. A l'aide du **Group Policy Object Editor**, créez un nouveau paquet d'installation dans le nœud **Configuration ordinateur**. Saisissez le chemin d'accès au fichier msi pour Kaspersky Security for Windows Server (de la Console de l'application) au format UNC (Universal Naming Convention).
6. Cochez la case **Toujours installer avec des droits élevés** du service Windows Installer aussi bien dans le nœud **Configuration ordinateur** que dans le nœud **Configuration utilisateur** du groupe sélectionné.
7. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Security for Windows Server est installé sur les ordinateurs du groupe après leur redémarrage.

## Actions à réaliser après l'installation de Kaspersky Security for Windows Server

Après l'installation de Kaspersky Security for Windows Server sur les serveurs protégés, il est conseillé de procéder immédiatement à la mise à jour des bases de l'application et de lancer une analyse rapide. Vous pouvez réaliser ces actions (cf. section "Actions à réaliser après l'installation de Kaspersky Security for Windows Server" à la page [59](#)) depuis la Console de l'application.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de

Kaspersky Security for Windows Server.

## Désinstallation de Kaspersky Security for Windows Server via des stratégies de groupe d'Active Directory

Si vous installez Kaspersky Security for Windows Server (ou la Console de l'application) sur le groupe de serveurs à l'aide d'une stratégie de groupe Active Directory, vous pourrez utiliser cette stratégie pour désinstaller Kaspersky Security for Windows Server (ou la console de l'application).

La suppression de l'application n'est possible que selon les paramètres de suppression par défaut.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

Si l'administration de l'application est protégée par mot de passe, il est impossible de désinstaller Kaspersky Security for Windows Server à l'aide de stratégies de groupe Active Directory.

► *Pour désinstaller Kaspersky Security for Windows Server (ou la Console de l'application) :*

1. Sur le contrôleur de domaine, sélectionnez l'unité d'organisation contenant les serveurs sur lesquels vous souhaitez désinstaller Kaspersky Security for Windows Server ou la Console de l'application.
2. Sélectionnez la stratégie créée pour l'installation de Kaspersky Security for Windows Server et dans **Editeur des stratégies de groupe**, nœud **Installation des logiciels (Configuration ordinateur > Configuration des programmes > Installation des logiciels)** ouvrez le menu contextuel du paquet d'installation de Kaspersky Security for Windows Server (de la console de l'application) et sélectionnez la commande **Toutes les tâches > Supprimer**.
3. Sélectionnez la méthode de suppression **Immediately uninstall the software from users and computers**.
4. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Security for Windows Server est supprimé des serveurs après leur redémarrage et avant l'ouverture de session dans Microsoft Windows.

## Vérification des fonctions de Kaspersky Security for Windows Server. Utilisation du virus d'essai EICAR

Cette section décrit le virus d'essai EICAR et explique comment l'utiliser pour confirmer le fonctionnement de la Protection en temps réel et de l'Analyse à la demande de Kaspersky Security for Windows Server.

## Dans cette section

A propos du virus d'essai EICAR.....	79
Vérification de la Protection en temps réel et de l'Analyse à la demande.....	80

## A propos du virus d'essai EICAR

Le virus d'essai vise à vérifier le fonctionnement des logiciels antivirus. Il a été développé par l'organisation The European Institute for Computer Antivirus Research (EICAR).

Le virus d'essai n'est pas un objet malveillant et il ne contient pas un code exécutable qui pourrait nuire à votre ordinateur mais les logiciels antivirus de la majorité des éditeurs le considèrent comme une menace.

Le fichier qui contient le virus d'essai s'appelle eicar.com. Vous pouvez le télécharger depuis le site Internet du projet EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Avant d'enregistrer le fichier dans un répertoire sur le disque dur de l'ordinateur, assurez-vous que la Protection des fichiers en temps réel est désactivée sur ce répertoire.

Le fichier eicar.com contient une ligne de texte. Pendant l'analyse, Kaspersky Security for Windows Server découvre la menace test dans cette ligne de texte, attribue l'état **Infecté** au fichier et le supprime. Les informations sur la menace découverte dans le fichier apparaissent dans la console de l'application, dans le journal d'exécution de la tâche.

Vous pouvez également utiliser le fichier eicar.com afin de voir comment Kaspersky Security for Windows Server désinfecte les objets infectés et comment il découvre les objets probablement infectés. Pour ce faire, ouvrez le fichier à l'aide d'un éditeur de texte, ajoutez au début de la ligne de texte un des préfixes repris au tableau ci-après et enregistrez le fichier sous un nouveau nom, par exemple eicar\_cure.com.

Pour s'assurer que Kaspersky Security for Windows Server traite le fichier eicar.com avec un préfixe, dans la section des paramètres de sécurité **Protection des objets**, indiquez la valeur **Tous les objets** pour les tâches Protection des fichiers en temps réel et Analyse à la demande de Kaspersky Security for Windows Server.

Tableau 7. Préfixe des fichiers EICAR

Préfixe	Etat du fichier après l'analyse et l'action de Kaspersky Security for Windows Server
Sans préfixe	Kaspersky Security for Windows Server attribue l'état <b>Infecté</b> à l'objet et le supprime.
SUSP-	Kaspersky Security for Windows Server attribue l'état <b>Probablement infecté</b> à l'objet découvert à l'aide de l'analyse heuristique et le supprime vu que les objets probablement infectés ne sont pas désinfectés.

Préfixe	Etat du fichier après l'analyse et l'action de Kaspersky Security for Windows Server
Sans préfixe	Kaspersky Security for Windows Server attribue l'état <b>Infecté</b> à l'objet et le supprime.
WARN-	Kaspersky Security for Windows Server attribue l'état <b>Probablement infecté</b> à l'objet (le code de l'objet correspond en partie à un code malveillant connu) et le supprime vu que les objets probablement infectés ne sont pas désinfectés.
CURE-	Kaspersky Security for Windows Server attribue l'état <b>Infecté</b> à l'objet et le désinfecte. Si la désinfection a réussi, tout le texte du fichier est remplacé par le mot "CURE".

## Vérification de la Protection en temps réel et de l'Analyse à la demande

Après l'installation de Kaspersky Security for Windows Server, vous pouvez confirmer que Kaspersky Security for Windows Server trouve les objets qui contiennent du code malveillant. Pour la vérification, vous pouvez utiliser un virus d'essai EICAR (cf. la section "A propos du virus d'essai EICAR" à la page [79](#)).

► Pour vérifier la fonction Protection en temps réel, procédez comme suit :

1. Téléchargez le fichier eicar.com du site Internet d'EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel ordinateur du réseau.

Avant d'enregistrer le fichier dans un dossier, assurez-vous que la Protection des fichiers en temps réel est désactivée pour ce dossier.

2. Si vous souhaitez également vérifier le fonctionnement des notifications des utilisateurs du réseau, assurez-vous que le service Windows Messenger de Microsoft est activé sur le serveur protégé et sur l'ordinateur sur lequel vous avez enregistré le fichier eicar.com.
3. Ouvrez la console de l'application.
4. Copiez le fichier eicar.com enregistré sur le disque local du serveur protégé selon une des méthodes suivantes :
  - Pour vérifier le fonctionnement des notifications via une fenêtre du service des terminaux, copiez le fichier eicar.com sur le serveur connecté à la console à l'aide du programme "Connexion au poste de travail distant" (Remote Desktop Connection).
  - Pour vérifier le fonctionnement des notifications via le service Windows Messenger, copiez le fichier eicar.com depuis l'ordinateur sur lequel vous l'avez enregistré via l'environnement de réseau de cet ordinateur.

La Protection des fichiers en temps réel fonctionne comme il se doit si les événements suivants se produisent :

- Le fichier eicar.com est supprimé du serveur protégé.
- Dans la Console de l'application, le journal d'exécution de la tâche reçoit l'état *Critique*. Le journal contient une nouvelle ligne qui reprend des informations au sujet d'une menace dans le fichier eicar.com. (Pour consulter le journal d'exécution de la tâche, développez, dans l'arborescence de la Console de l'application,

le nœud **Protection en temps réel du serveur**, sélectionnez la tâche **Protection des fichiers en temps réel** et, dans le panneau de détails du nœud, cliquez sur le lien **Ouvrir le journal d'exécution de la tâche**).

- Le message suivant du Service Windows Messenger de Microsoft apparaît sur l'ordinateur à partir duquel vous avez copié le fichier : Kaspersky Security for Windows Server a bloqué l'accès à <chemin du fichier sur l'ordinateur>\eicar.com sur l'ordinateur <nom de réseau de l'ordinateur> à <heure de l'événement>. Raison : menace détectée. Virus : EICAR-Test-File. Nom d'utilisateur : <nom d'utilisateur>. Nom de l'ordinateur : <nom réseau de l'ordinateur d'où vous avez copié le fichier>.

Assurez-vous que le service Windows Messenger de Microsoft fonctionne sur l'ordinateur d'où vous avez copié le fichier eicar.com.

► Pour vérifier la fonction *Analyse à la demande*, procédez comme suit :

- Téléchargez le fichier eicar.com du site Internet d'EICAR [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel ordinateur du réseau.

Avant d'enregistrer le fichier dans un dossier, assurez-vous que la Protection des fichiers en temps réel est désactivée pour ce dossier.

- Ouvrez la console de l'application.
- Exécutez les actions suivantes :
  - Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
  - Sélectionnez le nœud enfant **Analyse des zones critiques**.
  - Sous l'onglet **Configuration de la zone d'analyse**, ouvrez le menu contextuel du nœud **Réseau**, puis choisissez **Ajouter un fichier de réseau**.
  - Saisissez le chemin d'accès réseau au fichier eicar.com sur l'ordinateur distant au format UNC (Universal Naming Convention).
  - Cochez la case afin d'inclure le chemin de réseau dans la zone d'analyse.
  - Lancez la tâche Analyse des zones critiques.

L'analyse à la demande fonctionne correctement si les conditions suivantes sont remplies :

- Le fichier eicar.com est supprimé du disque dur de l'ordinateur.
- Dans la Console de l'application, le journal d'exécution de la tâche reçoit l'état *Critique*. Le journal d'exécution de la tâche Analyse des zones critiques contient une nouvelle ligne qui reprend des informations au sujet d'une menace dans le fichier eicar.com. (Pour consulter le journal d'exécution de la tâche, développez, dans l'arborescence de la Console de l'application, le nœud **Analyse à la demande**, sélectionnez la tâche Analyse des zones critiques et dans le panneau de détails du nœud, cliquez sur le lien **Ouvrir le journal d'exécution de la tâche**).

# Interface de l'application

Il est possible de contrôler Kaspersky Security for Windows Server à l'aide d'un plug-in d'administration et de la Console de l'application locale.

Les actions qui peuvent être exécutées via l'interface de la Console de l'application sont décrites dans la section Utilisation de la Console de l'application (cf. section "Utilisation de la Console de Kaspersky Security for Windows Server" à la page [143](#)).

L'interface de la console d'administration de Kaspersky Security Center sert à exécuter des actions avec le plug-in d'administration. L'*aide de Kaspersky Security Center* fournit des informations détaillées sur l'interface de Kaspersky Security Center.



# Licence de l'application

Cette section présente les principales notions relatives à la licence de l'application.

## Contenu du chapitre

A propos du Contrat de licence utilisateur final .....	<a href="#">83</a>
A propos de la licence .....	<a href="#">84</a>
A propos du certificat de licence.....	<a href="#">84</a>
A propos de la clé .....	<a href="#">85</a>
A propos du fichier clé .....	<a href="#">85</a>
A propos du code d'activation.....	<a href="#">85</a>
A propos de l'abonnement.....	<a href="#">86</a>
A propos de la collecte des données.....	<a href="#">86</a>
Activation de l'application à l'aide d'une clé de licence .....	<a href="#">89</a>
Consultation des informations sur la licence active.....	<a href="#">89</a>
Restriction des fonctions à l'expiration de la licence .....	<a href="#">92</a>
Renouvellement de la licence.....	<a href="#">93</a>
Suppression d'une clé.....	<a href="#">93</a>

## A propos du Contrat de licence utilisateur final

Le *Contrat de Licence Utilisateur Final* est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement les conditions du Contrat de licence utilisateur final avant de commencer à utiliser l'application.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final, en utilisant les moyens suivants :

- Lors de l'installation de Kaspersky Security for Windows Server
- En lisant le document license.txt. Ce document est inclus dans le kit de distribution de l'application.

Vous acceptez les conditions du Contrat de licence utilisateur final, en confirmant votre accord avec le texte du Contrat de licence utilisateur final lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence utilisateur final, vous devez interrompre l'installation de l'application et vous ne pouvez pas utiliser l'application.

## A propos de la licence

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

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application dans le respect des dispositions du Contrat de licence utilisateur final ;
- Obtention du Support Technique.

Une licence *commerciale* est une licence payante octroyée à l'achat de l'application. A l'expiration de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases de l'application n'est plus disponible). Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky Security for Windows Server, il faut renouveler la validité de la licence commerciale.

La fonctionnalité disponible de l'application dans le cadre de la licence commerciale dépend du choix du produit. Le produit sélectionné est indiqué dans le certificat de licence (cf. section "A propos du certificat de licence" à la page 84). Vous trouverez des informations sur les produits disponibles sur le site Internet de Kaspersky Lab à l'adresse <https://www.kaspersky.fr/small-to-medium-business-security>.

Il est conseillé de renouveler la validité de la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre toutes les menaces.

Assurez-vous que la période d'activation de la clé additionnelle que vous ajoutez possède une date d'expiration ultérieure à celle de la clé active.

Vous ne pouvez pas utiliser d'abonnement comme clé additionnelle.

## A propos du certificat de licence

Un *certificat de licence* est un document qui vous est remis avec le fichier clé ou le code d'activation (le cas échéant).

Le certificat de licence reprend les informations suivantes relatives à la licence octroyée :

- Numéro de la commande ;
- Informations sur l'utilisateur qui a obtenu la licence ;
- Informations sur l'application qui peut être activée à l'aide de la licence octroyée ;
- Limite du nombre d'unités sous licence (par exemple, les appareils sur lesquels l'application peut être utilisée sous les termes de la licence fournie) ;
- Date de début de validité de la licence ;
- Date d'expiration de la licence ou dispositions de la licence
- Type de licence

## A propos de la clé

La *clé* est une séquence d'octets qui permet d'activer l'application en vue de son utilisation dans le respect des dispositions du Contrat de licence utilisateur final. La clé est générée par les experts de Kaspersky Lab.

Vous pouvez ajouter une clé à l'application en utilisant un fichier clé. La clé apparaît dans l'interface de l'application sous la forme d'une séquence alphanumérique unique après que vous l'avez ajoutée à l'application.

La clé peut être bloquée par Kaspersky Lab en cas de non-respect du Contrat de licence utilisateur final. Si la clé est bloquée, il faudra en ajouter une autre pour pouvoir utiliser l'application.

Une clé peut être active ou additionnelle.

*Clé active* est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour une licence commerciale ou d'essai peut être ajoutée en tant que clé active. L'application ne peut pas contenir plus d'une clé active.

La *Clé additionnelle* est une clé qui confirme le droit d'utilisation de l'application, non utilisée au moment actuel. Une clé additionnelle devient automatiquement une clé active à l'expiration de la validité de la licence associée à la clé active en cours. Une clé additionnelle ne peut être ajoutée que si une clé active existe.

## A propos du fichier clé

Un *fichier clé* est un fichier portant l'extension .key qui vous est remis par Kaspersky Lab. Les fichiers clé permet d'ajouter une clé de licence pour activer l'application.

Le fichier clé est envoyé à l'adresse email que vous avez indiquée au moment de l'achat de Kaspersky Security for Windows Server ou après avoir sollicité une version d'essai de Kaspersky Security for Windows Server.

Pour activer l'application à l'aide du fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky Lab.

En cas de suppression accidentelle du fichier clé, vous pouvez le récupérer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour récupérer un fichier clé, réalisez une des actions suivantes :

- Contactez le vendeur de la licence.
- Obtenez un fichier clé via le site Internet de Kaspersky Lab (<https://keyfile.kaspersky.com/en/>) en utilisant votre code d'activation.

## A propos du code d'activation

Un *code d'activation* est une séquence unique de 20 lettres et chiffres. Vous devez entrer un code d'activation afin d'ajouter une clé pour activer Kaspersky Security for Windows Server. Vous recevez le code d'activation à l'adresse email que vous avez fournie à l'achat de Kaspersky Security for Windows Server.

Pour activer l'application avec un code d'activation, vous avez besoin d'un accès Internet pour pouvoir vous connecter aux serveurs d'activation de Kaspersky Lab.

Si vous avez perdu votre code d'activation après l'installation de l'application, il peut être récupéré. Vous aurez

besoin du code d'activation pour ouvrir un compte d'entreprise Kaspersky par exemple. Pour récupérer votre code d'activation, contactez le Support Technique de Kaspersky Lab.

## A propos de l'abonnement

Un *abonnement* est une séquence unique de 20 lettres et chiffres. Il donne le droit d'utiliser l'application dans le cadre des paramètres sélectionnés (date de fin de l'abonnement, nombre d'appareils protégés). Un abonnement Kaspersky Security for Windows Server peut être enregistré auprès d'un fournisseur de services (par exemple, votre FAI). Vous pouvez prolonger un abonnement manuellement ou automatiquement. Vous pouvez également suspendre, puis reprendre un abonnement. La gestion de l'abonnement est disponible via le fournisseur de services ; vous ne pouvez pas gérer un abonnement indépendamment.

Les options de gestion des abonnements dépendent du fournisseur de services. Le fournisseur de services peut offrir une *période de grâce* pour le renouvellement d'un abonnement.

Une période de grâce est un intervalle au cours duquel la fonctionnalité de l'application reste inchangée entre la fin d'un abonnement et son renouvellement.

Un abonnement peut être *limité* ou *illimité*.

Un abonnement limité offre une durée de licence limitée et ne se renouvelle pas automatiquement.

Un abonnement illimité est renouvelé automatiquement sans votre participation si le paiement est effectué à temps, et ne possède pas de date d'expiration fixe.

Le statut d'un abonnement s'affiche dans le volet détails du nœud **Kaspersky Security** et est automatiquement mis à jour toutes les heures. Vous ne pouvez pas mettre à jour manuellement l'état d'un abonnement.

Les codes d'activation obtenus par abonnement ne peuvent pas être utilisés pour activer les versions précédentes de l'application.

## A propos de la collecte des données

Le contrat de licence de Kaspersky Security for Windows Server, notamment la section intitulée "Conditions du traitement des données", spécifie les conditions, la responsabilité et la procédure de traitement des données indiquées dans ce Guide. Avant d'accepter le contrat de licence, révisez attentivement ses conditions, ainsi que tous les documents liés au contrat de licence.

Les données que vous envoyez à Kaspersky Lab lorsque vous utilisez l'application sont protégées et traitées conformément à la Politique de confidentialité disponible à l'adresse [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

En acceptant les conditions du contrat de licence, vous acceptez d'envoyer automatiquement les données suivantes à Kaspersky Lab :

- Pour prendre en charge le mécanisme de réception de mises à jour : informations sur l'application installée et son activation : identifiant de l'application en cours d'installation et version complète, y compris le numéro de version, le type et l'identifiant de licence, identifiant d'installation, identifiant de la tâche de mise à jour.
- Pour accéder aux articles de la base de connaissances en cas d'erreurs de l'application (service de

redirection) : informations sur le type d'application et de lien, notamment le nom, l'environnement local et le numéro de version complète de l'application, type de lien de redirection et identifiant d'erreur.

- Pour gérer les confirmations du traitement des données : informations sur l'état d'acceptation des contrats de licence et des autres documents, qui stipulent les conditions de transfert des données : identifiant et version du contrat de licence ou des autres documents, comprenant les conditions acceptées ou refusées du traitement des données, attribut désignant l'action de l'utilisateur (confirmation ou rappel de l'acceptation des conditions) ; date et heure des changements d'état de l'acceptation des conditions de traitement des données.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final, en utilisant les moyens suivants :

- Lors de l'installation, l'assistant Installation de Kaspersky Security for Windows Server affiche le texte intégral du Contrat de licence à l'étape de l'acceptation des dispositions de celui-ci.
- Ce texte peut également être consulté à tout moment dans le fichier TXT (licence.txt). Ce fichier figure dans le kit de distribution de Kaspersky Security for Windows Server, aux côtés des fichiers d'installation de l'application.

### Traitement des données locales

Tout en exécutant les fonctions principales de l'application décrites dans ce Guide, Kaspersky Security for Windows Server traite et stocke en local une séquence de données sur le serveur protégé.

Kaspersky Security for Windows Server traite et store en local les données suivantes :

- Informations sur les fichiers analysés et les objets détectés, par exemple les noms et attributs des fichiers traités, et les chemins d'accès complets à ces derniers sur les supports analysés, types de fichier, actions effectuées sur les fichiers analysés, comptes des utilisateurs effectuant des actions sur le réseau protégé ou sur le serveur protégé, noms et données sur les périphériques analysés, informations sur les processus exécutés sur le système, sommes de contrôle (MD5, SHA-256) et horodatage des processus exécutés sur le système, attributs de certificat numérique, données relatives aux scripts exécutés.
- informations sur l'activité et les paramètres du système d'exploitation, par exemple, paramètres du pare-feu Windows, entrées du journal des événements Windows, noms des comptes utilisateur, lancements des fichiers exécutables, leurs sommes de contrôle et attributs ;
- informations sur l'activité du réseau locale, y compris les adresses IP des ordinateurs clients bloqués.
- Informations relatives aux adresses Internet analysées et aux fichiers téléchargés, par exemple, l'adresse Internet et les adresses IP où le téléchargement a débuté, la page Internet de téléchargement, l'identifiant du protocole et le numéro d'un port de connexion, l'attribut de dangerosité d'une adresse, les attributs et la taille du fichier et ses sommes de contrôle (MD5, SHA-256), les sommes de contrôle (MD5, SHA-256) du fichier exécutable de processus ayant téléchargé le fichier, un attribut qui indique si la détection a eu lieu pendant le débogage, l'identifiant du protocole de connexion, le numéro de port utilisé, les adresses Internet en cours d'analyse, le nom d'un fichier analysé, les données du certificat Internet.

Kaspersky Security for Windows Server traite et stocke les données, ce qui fait partie de la fonctionnalité de base de l'application, notamment pour enregistrer dans le journal les événements de l'application et recevoir des données de diagnostic. Les données traitées en local sont en outre protégées conformément aux paramètres configurés et appliqués de l'application.

Kaspersky Security for Windows Server vous permet de configurer le niveau de protection des données traitées en local : vous pouvez modifier les droits d'accès des utilisateurs aux données du processus, modifier les périodes de conservation de ces données, désactiver entièrement ou partiellement la fonctionnalité qui implique l'enregistrement des événements dans le journal des données et modifier le chemin et les attributs du dossier où les données sont enregistrées.

Vous trouverez des informations détaillées sur la configuration des fonctionnalités de l'application qui impliquent le traitement des données et les paramètres par défaut du stockage des données traitées dans les sections correspondantes de ce Guide.

Les données traitées dans l'application en local ne sont pas automatiquement envoyées à Kaspersky Lab ou à d'autres systèmes tiers.

Par défaut, toutes les données traitées localement par l'application en cours de fonctionnement sont retirées après la suppression de Kaspersky Security for Windows Server du serveur.

Font exception les fichiers contenant des informations de diagnostic (fichiers de trace et dump) et les événements de l'application dans le journal des événements Windows. Il est recommandé de supprimer manuellement ces fichiers.

Vous trouverez des informations détaillées sur l'utilisation de fichiers contenant les données de diagnostic de l'application dans les sections correspondantes de ce guide.

Vous pouvez supprimer les fichiers journaux des événements Windows contenant les événements de l'application Kaspersky Security for Windows Server via les moyens standard du système d'exploitation.

#### Traitement des données locales à l'aide des composants auxiliaires de l'application

Le paquet d'installation de Kaspersky Security for Windows Server comprend des composants auxiliaires de l'application qui peuvent être installés sur votre serveur ou ordinateur même si Kaspersky Security for Windows Server n'est pas installé dessus. Ces composants auxiliaires sont les suivants :

- Console de l'application. Ce composant est inclus dans les Outils d'administration de Kaspersky Security for Windows Server et représenté par un composant logiciel enfichable Microsoft Management Console.
- Plug-in du client de messagerie Microsoft Outlook. Ce composant assure la recherche du virus dans les emails.
- Plug-in d'administration. Ce composant assure une intégration complète avec l'application Kaspersky Security Center.

Tout en assurant les fonctions principales de l'application décrite dans ce Guide, les composants auxiliaires de l'application traitent et stockent en local un ensemble de données sur le serveur où ils sont installés même s'ils sont installés séparément de Kaspersky Security for Windows Server.

Les composants de l'application traitent en local et stockent les données suivantes :

- Console de l'application : nom, sous forme de chaîne, du serveur hébergeant Kaspersky Security for Windows Server (adresse IP ou nom de domaine) auquel la Console de l'application s'est connectée à distance pour la dernière fois ; paramètres d'affichage configurés dans le composant logiciel enfichable Microsoft Management Console ; données concernant le dernier dossier dans lequel l'utilisateur a sélectionné des objets via la Console de l'application (à l'aide d'une boîte de dialogue ouverte via le bouton **Parcourir**). Les fichiers de trace de la Console de l'application peuvent également contenir les données suivantes : nom du serveur hébergeant l'application Kaspersky Security for Windows Server auquel la connexion à distance a été effectuée, le nom du compte utilisateur sous lequel la connexion à distance a été établie.
- Le Plug-in du client de messagerie Microsoft Outlook stocke les données uniquement dans des fichiers de trace. Les fichiers de trace du complément du client de messagerie Microsoft Outlook peut contenir les informations suivantes : données des champs des messages électroniques ("De", "A", "Objet"), métadonnées des corps des messages et des pièces jointes (type, taille, nom de la pièce jointe).
- Le Plug-in d'administration peut traiter et stocker temporairement des données traitées par Kaspersky Security for Windows Server ; par exemple les paramètres configurés des tâches et des composants de l'application, les paramètres des stratégies de Kaspersky Security Center, les données envoyées dans les

listes de réseau.

Les données traitées par les composants auxiliaires ne sont pas automatiquement envoyées à Kaspersky Lab ou à d'autres systèmes tiers.

Par défaut, toutes les données traitées en local par les composants auxiliaires de l'application en cours de fonctionnement sont supprimées après la désinstallation de ces composants.

Font exception les fichiers de trace des composants auxiliaires de l'application. Il est recommandé de les supprimer manuellement.

Vous trouverez des informations détaillées sur l'utilisation de fichiers contenant les données de diagnostic des composants auxiliaires de l'application dans les sections correspondantes de ce guide.

## Activation de l'application à l'aide d'une clé de licence

Vous pouvez activer Kaspersky Security for Windows Server en appliquant une clé.

Si Kaspersky Security for Windows Server possède déjà une clé active et si vous ajoutez une autre clé en tant que clé active, la nouvelle clé remplacera l'ancienne. La clé ajoutée antérieurement est supprimée.

Si Kaspersky Security for Windows Server possède déjà une clé additionnelle et si vous ajoutez une autre clé en tant que clé additionnelle, la nouvelle clé remplacera l'ancienne. La clé additionnelle ajoutée antérieurement est supprimée.

Si une clé additionnelle et une clé active avaient déjà été ajoutées à Kaspersky Security for Windows Server et que vous ajoutez une nouvelle clé en tant que clé active, cette nouvelle clé remplace la clé active antérieure et la clé additionnelle n'est pas supprimée.

► *Pour activer Kaspersky Security for Windows Server :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Licence**.
2. Dans le panneau de détails du nœud **Licence**, cliquez sur le lien **Ajouter une clé**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir** et sélectionnez le fichier clé portant l'extension key.

Vous pouvez aussi ajouter une clé en tant que clé additionnelle. Pour ce faire, cochez la case **Utiliser en tant que clé additionnelle**.

4. Cliquez sur le bouton **OK**.

La clé sélectionnée sera appliquée. L'information sur la clé ajoutée s'affiche dans le nœud **Licence**.

## Consultation des informations sur la licence active

### Consultation des informations sur la licence

Les informations sur la licence active s'affichent dans le panneau de détails du nœud **Kaspersky Security** de la console de l'application. Une clé peut afficher les états suivants :

- **Vérification de l'état de la clé** : Kaspersky Security for Windows Server analyse le fichier clé ou le code



d'activation appliqué, puis attend une réponse concernant l'état de la clé actuelle.

- **Date d'expiration de la licence** : Kaspersky Security for Windows Server est actif jusqu'à la date et l'heure indiquées. L'état de la clé est mis en évidence en jaune dans les cas suivants :
  - Il reste 14 jours avant l'expiration de la licence et aucun fichier clé additionnel n'a été appliqué.
  - La clé ajoutée est inscrite sur la liste noire et va bientôt être bloquée.
- **L'application n'a pas été activée** : Kaspersky Security for Windows Server n'a pas été activé car aucun fichier clé ou aucun code d'activation n'a été appliqué. L'état est mis en évidence en rouge.
- **Licence expirée** : Kaspersky Security for Windows Server n'est pas actif car la licence a expiré. L'état est mis en évidence en rouge.
- **Violation du Contrat de licence utilisateur final** : Kaspersky Security for Windows Server n'est pas activé en raison d'une violation des conditions du Contrat de licence utilisateur final (cf. section "A propos du Contrat de licence utilisateur final" à la page [83](#)). L'état est mis en évidence en rouge.
- **Clé placée dans la liste noire** : la clé ajoutée a été bloquée et inscrite sur la liste noire par les experts de Kaspersky Lab, par exemple, en cas d'utilisation d'une clé par des tiers pour l'activation illicite d'une application. L'état est mis en évidence en rouge.
- **Abonnement suspendu** : l'abonnement a été temporairement suspendu. L'état est mis en évidence en rouge. Vous pouvez renouveler l'abonnement à tout moment.

### Consultation des informations sur la licence active

► Pour consulter les informations sur la licence active, procédez comme suit :

Dans l'arborescence de la console de l'application, développez le nœud **Licence**.

Les informations générales relatives à la licence active apparaissent dans le panneau de détails du nœud **Licence** (cf. tableau ci-dessous).

Tableau 8. Informations générales sur la licence dans le nœud Licence

Champ	Description
<b>Code d'activation</b>	Le code d'activation. Le champ se remplit si vous activez l'application à l'aide d'un code d'activation.
<b>Etat de l'activation</b>	Informations sur l'état de l'activation de l'application. La colonne <b>Activation</b> du panneau de détails du nœud <b>Licence</b> peut afficher les états suivants : <ul style="list-style-type: none"> <li>• <b>Appliqué</b> : si vous avez activé l'application à l'aide d'un code d'activation ou d'un fichier clé.</li> <li><b>Activation</b> : si vous avez appliqué un code d'activation pour activer l'application et que le processus est toujours en cours. L'état devient <i>Appliqué</i> à la fin de l'activation de l'application et le contenu du panneau de détails du nœud est mis à jour.</li> <li>• <b>Erreur d'activation</b> : apparaît en cas d'échec de l'activation de l'application. Vous pouvez voir la cause de l'échec de l'activation dans le journal d'exécution de la tâche.</li> </ul>
<b>Clé</b>	La clé utilisée pour activer l'application.
<b>Type de licence</b>	Type de licence : commerciale ou d'essai.
<b>Date d'expiration</b>	Date et heure d'expiration de la licence associée à la clé active.

Champ	Description
<b>Etat du code d'activation ou de la clé</b>	Etat du code d'activation ou de la clé : actif ou additionnel.

► *Pour voir les informations détaillées relatives à la licence, procédez comme suit :*

Pour le nœud **Licence**, ouvrez le menu contextuel de la ligne des informations sur la licence que vous voulez examiner, puis choisissez l'option **Propriétés**.

Dans la fenêtre **Propriétés** : **<Etat du code d'activation ou de la clé>**, l'onglet **Général** reprend les détails relatifs à la licence active et l'onglet **Avancé** contient les informations relatives au client et les coordonnées de Kaspersky Lab ou du partenaire chez qui vous avez acheté Kaspersky Security for Windows Server (cf. tableau ci-dessous).

Tableau 9. Détails relatifs à la licence dans la fenêtre Propriétés : <Etat du code d'activation ou de la clé>

Champ	Description
<b>Onglet Général</b>	
<b>Clé</b>	La clé utilisée pour activer l'application.
<b>Date d'ajout de la clé</b>	Date d'ajout de la clé dans l'application.
<b>Type de licence</b>	Type de licence : commerciale ou d'essai.
<b>Expire dans (jours)</b>	Nombre de jours restants avant l'expiration de la licence associée à la clé active.
<b>Date d'expiration</b>	Date et heure d'expiration de la licence associée à la clé active. Si vous activez l'application selon un abonnement illimité, la valeur <i>Illimité</i> apparaît dans le champ. Si Kaspersky Security for Windows Server ne parvient pas à déterminer la date d'expiration de la licence, la valeur <i>Inconnue</i> apparaît dans le champ.
<b>Application</b>	Le nom de l'application activée à l'aide du fichier clé ou du code d'activation.
<b>Restrictions d'utilisation de la clé</b>	Restrictions sur l'utilisation de la clé (le cas échéant).
<b>Accès à l'assistance technique</b>	Indique si la licence prévoit une assistance technique offerte par Kaspersky Lab ou par ses partenaires.
<b>Onglet Avancé</b>	
<b>Informations relatives à la licence</b>	Numéro de la licence en cours
<b>Informations relatives au support</b>	Coordonnées de Kaspersky Lab ou du partenaire qui offre le Support Technique. Le champ peut être vide en l'absence de Support Technique.
<b>Informations relatives au détenteur</b>	Informations relatives au titulaire de la licence : nom du client ou de l'organisation pour laquelle une licence a été achetée.

## Restriction des fonctions à l'expiration de la licence

Une fois que la licence active arrive à échéance, les restrictions suivantes sont appliquées aux composants fonctionnels :

- Toutes les tâches sont arrêtées, à l'exception des tâches Protection des fichiers en temps réel, Analyse à la demande et Vérification de l'intégrité de l'application.
- Aucune tâche ne peut être lancée, à l'exception de la Protection des fichiers en temps réel, de l'Analyse à la demande et de la Vérification de l'intégrité de l'application. Ces tâches sont toujours opérationnelles, mais font intervenir les anciennes bases antivirus.
- La fonction Protection contre les exploits est limitée :

- Les processus sont protégés jusqu'à leur redémarrage.
- Il est impossible d'ajouter de nouveaux processus à la zone de protection.

Les autres fonctions (référentiels, journaux, informations de diagnostic) sont toujours disponibles.

## Renouvellement de la licence

Par défaut Kaspersky Security for Windows Server signale l'échéance prochaine de la validité de la licence 14 jours avant sa date d'expiration. Dans ce cas, l'état **Date d'expiration de la licence** est mis en évidence en jaune dans le volet des détails du nœud **Kaspersky Security**.

Vous pouvez renouveler la licence avant sa date d'expiration grâce à l'ajout d'un code d'activation ou d'un fichier clé additionnel. Ainsi, la protection du serveur ne sera pas interrompue entre la fin de la validité de la licence active et l'activation de l'application à l'aide d'une nouvelle licence.

► *Pour renouveler la licence, procédez comme suit :*

1. Achetez un nouveau code d'activation de l'application ou un nouveau fichier clé.
2. Dans l'arborescence de la console de l'application, développez le nœud **Licence**.
3. Dans le panneau de détails du nœud **Licence**, exécutez une des actions suivantes :
  - Si vous souhaitez renouveler la licence à l'aide d'une clé additionnelle :
    - a. Cliquez sur le lien **Ajouter une clé**.
    - b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**, puis sélectionnez le nouveau fichier clé portant l'extension key.
    - c. Cochez la case **Utiliser en tant que clé additionnelle**.
  - Si vous souhaitez renouveler la licence à l'aide d'un code d'activation :
    - a. Cliquez sur le lien **Ajouter un code d'activation**.
    - b. Dans la fenêtre qui s'ouvre, saisissez le code d'activation.
    - c. Cochez la case **Utiliser en tant que clé additionnelle**.

L'application d'un code d'activation requiert une connexion à Internet.

4. Cliquez sur le bouton **OK**.

La clé additionnelle est ajoutée et appliquée automatiquement à l'expiration de la licence de Kaspersky Security for Windows Server.

## Suppression d'une clé

Vous pouvez supprimer une clé que vous avez ajoutée.

Si Kaspersky Security for Windows Server possède une clé additionnelle et que vous supprimez la clé active, la clé additionnelle devient automatiquement la clé active.

Si vous supprimez la clé qui avait été ajoutée, vous pourrez la restaurer après avoir appliqué à nouveau le fichier clé.

► *Pour supprimer la clé ajoutée, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Licence**.
2. Dans le tableau contenant les informations relatives aux clés ajoutées qui figure dans le panneau de détails du nœud **Licence**, sélectionnez la clé que vous souhaitez supprimer.
3. Dans le menu contextuel de la ligne contenant les informations sur la clé sélectionnée, choisissez l'option **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

La clé sélectionnée sera supprimée.

# Utilisation du plug-in d'administration

Cette section fournit des informations sur le plug-in d'administration de Kaspersky Security for Windows Server et décrit la procédure d'administration de l'application installée sur un serveur protégé ou sur un groupe de serveurs.

## Contenu du chapitre

Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center .....	<a href="#">95</a>
Administration des paramètres de l'application .....	<a href="#">97</a>
Création et configuration des stratégies .....	<a href="#">116</a>
Création et configuration de tâches via Kaspersky Security Center .....	<a href="#">124</a>
Génération de rapports dans Kaspersky Security Center .....	<a href="#">140</a>

## Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center

Vous pouvez réaliser l'administration centralisée de plusieurs serveurs dotés de Kaspersky Security for Windows Server et inclus dans un groupe d'administration via le plug-in d'administration de Kaspersky Security for Windows Server. Kaspersky Security Center permet également de configurer séparément les paramètres de fonctionnement de chaque serveur au sein du groupe d'administration.

Le *groupe d'administration* est créé manuellement du côté de Kaspersky Security Center et contient plusieurs serveurs dotés de Kaspersky Security for Windows Server et pour lesquels vous souhaitez configurer des paramètres d'administration et de protection identiques. Pour en savoir plus sur l'utilisation de groupes d'administration, consultez le *Système d'aide de Kaspersky Security Center*.

Les paramètres de l'application pour un ordinateur ne peuvent être configurés si le fonctionnement de Kaspersky Security for Windows Server sur ce serveur est contrôlé par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Security for Windows Server depuis Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center.** Les stratégies de Kaspersky Security Center permettent de configurer à distance des paramètres de protection unique pour un groupe de serveurs. Les paramètres de la tâche, définis dans la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la console de l'application ou à distance dans la fenêtre **Propriétés : <nom de l'ordinateur>** de Kaspersky Security Center.

Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches Protection en temps réel, Contrôle de l'activité locale, Protection des stockages réseau, les paramètres du lancement des tâches système planifiées et les paramètres d'usage du profil.

- **A l'aide de tâches de groupe de Kaspersky Security Center.** Les tâches de groupe de Kaspersky Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai

d'exécution limité pour un groupe de serveurs.

- Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche de Génération des règles du Contrôle du lancement des applications.
- **A l'aide de tâches pour une sélection de périphériques.** Les tâches pour une sélection de périphériques permettent de configurer à distance des paramètres de tâches communs ayant un délai d'exécution limité pour les serveurs qui ne figurent dans aucun des groupes d'administration créés.
- **A l'aide de la fenêtre de configuration des paramètres d'un ordinateur.** La fenêtre **Propriétés : <nom de l'ordinateur>** permet de configurer à distance les paramètres d'une tâche pour un serveur unique appartenant au groupe d'administration. Vous pouvez configurer ainsi les paramètres généraux de fonctionnement de l'application et les paramètres de toutes les tâches de Kaspersky Security for Windows Server, si le serveur sélectionné n'est pas contrôlé par une stratégie active de Kaspersky Security Center.

Kaspersky Security Center permet de configurer les paramètres de l'application, les possibilités additionnelles et le fonctionnement des journaux et notifications. Vous pouvez configurer ces paramètres aussi bien pour un groupe de serveur que pour un seul.



## Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Security for Windows Server dans Kaspersky Security Center.

### Contenu du chapitre

Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center .....	<a href="#">97</a>
Navigation .....	<a href="#">98</a>
Configuration des paramètres généraux de l'application dans Kaspersky Security Center.....	<a href="#">99</a>
Configuration des paramètres de la quarantaine et de la Sauvegarde dans Kaspersky Security Center .....	<a href="#">105</a>
Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués .....	<a href="#">106</a>
A propos de la configuration des journaux et notifications .....	<a href="#">108</a>

## Gestion de Kaspersky Security for Windows Server à partir de Kaspersky Security Center

Vous pouvez réaliser l'administration centralisée de plusieurs serveurs dotés de Kaspersky Security for Windows Server et inclus dans un groupe d'administration via le plug-in d'administration de Kaspersky Security for Windows Server. Kaspersky Security Center permet également de configurer séparément les paramètres de fonctionnement de chaque serveur au sein du groupe d'administration.

Le *groupe d'administration* est créé manuellement du côté de Kaspersky Security Center et contient plusieurs serveurs dotés de Kaspersky Security for Windows Server et pour lesquels vous souhaitez configurer des paramètres d'administration et de protection identiques. Pour en savoir plus sur l'utilisation de groupes d'administration, consultez le *Système d'aide de Kaspersky Security Center*.

Les paramètres de l'application pour un ordinateur ne peuvent être configurés si le fonctionnement de Kaspersky Security for Windows Server sur ce serveur est contrôlé par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Security for Windows Server depuis Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center.** Les stratégies de Kaspersky Security Center permettent de configurer à distance des paramètres de protection unique pour un groupe de serveurs. Les paramètres de la tâche, définis dans la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la console de l'application ou à distance dans la fenêtre **Propriétés : <nom de l'ordinateur>** de Kaspersky Security Center.

Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches Protection en temps réel, Contrôle de l'activité locale, Protection des stockages réseau, les paramètres du lancement des tâches système planifiées et les paramètres d'usage du profil.

- **A l'aide de tâches de groupe de Kaspersky Security Center.** Les tâches de groupe de Kaspersky

Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai d'exécution limité pour un groupe de serveurs.

- Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche de Génération des règles du Contrôle du lancement des applications.
- **A l'aide de tâches pour une sélection de périphériques.** Les tâches pour une sélection de périphériques permettent de configurer à distance des paramètres de tâches communs ayant un délai d'exécution limité pour les serveurs qui ne figurent dans aucun des groupes d'administration créés.
- **A l'aide de la fenêtre de configuration des paramètres d'un ordinateur.** La fenêtre **Propriétés : <nom de l'ordinateur>** permet de configurer à distance les paramètres d'une tâche pour un serveur unique appartenant au groupe d'administration. Vous pouvez configurer ainsi les paramètres généraux de fonctionnement de l'application et les paramètres de toutes les tâches de Kaspersky Security for Windows Server, si le serveur sélectionné n'est pas contrôlé par une stratégie active de Kaspersky Security Center.

Kaspersky Security Center permet de configurer les paramètres de l'application, les possibilités additionnelles et le fonctionnement des journaux et notifications. Vous pouvez configurer ces paramètres aussi bien pour un groupe de serveur que pour un seul.

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Accès aux paramètres généraux via la stratégie.....	<a href="#">98</a>
Accès aux paramètres généraux dans la fenêtre des propriétés de l'application .....	<a href="#">99</a>

## Accès aux paramètres généraux via la stratégie

► *Pour accéder aux paramètres de l'application de Kaspersky Security for Windows Server via la stratégie :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Paramètres de l'application**.
6. Cliquez sur le bouton **Configuration** dans la sous-section du paramètres que vous souhaitez configurer.

## Accès aux paramètres généraux dans la fenêtre des propriétés de l'application

► Pour ouvrir la fenêtre des propriétés de Kaspersky Security for Windows Server pour un seul serveur :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <nom du serveur>** à l'aide d'une des méthodes suivantes :
  - Double-clic sur le nom du serveur protégé.
  - Sélectionnez l'option **Propriétés** dans le menu contextuel du serveur protégé.

La fenêtre **Propriétés : <nom du serveur>** s'ouvre.

5. Dans la section **Applications**, sélectionnez **Kaspersky Security for Windows Server**.
6. Cliquez sur le bouton **Propriétés**.

La fenêtre de **configuration de l'application Kaspersky Security for Windows Server** s'ouvre.

7. Sélectionnez la section **Paramètres de l'application**.

## Configuration des paramètres généraux de l'application dans Kaspersky Security Center

Vous pouvez configurer les paramètres généraux de Kaspersky Security for Windows Server depuis Kaspersky Security Center pour un groupe de serveurs ou pour un serveur individuel.

### Dans cette section

Configuration de la montée en puissance et de l'interface dans Kaspersky Security Center .....	<a href="#">99</a>
Configuration des paramètres de sécurité dans Kaspersky Security Center .....	<a href="#">101</a>
Configuration des paramètres de connexion dans Kaspersky Security Center .....	<a href="#">102</a>
Configuration du lancement planifié des tâches locales du système prédéfinies .....	<a href="#">104</a>

## Configuration de la montée en puissance et de l'interface dans Kaspersky Security Center

► Pour configurer les paramètres d'optimisation et l'interface de l'application, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une

stratégie" à la page [123](#)).

- Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Paramètres de l'application** du groupe **Montée en puissance et interface**, cliquez sur **Configuration**.
5. Sous l'onglet **Général** de la fenêtre **Paramètres avancés de l'application**, configurez les paramètres suivants :
  - La section **Paramètres d'optimisation** permet de configurer les paramètres qui définissent le nombre de processus utilisés par Kaspersky Security for Windows Server.
    - **Détecter automatiquement les paramètres d'optimisation.**

Kaspersky Security for Windows Server régit automatiquement le nombre de processus utilisés.

Cette valeur est définie par défaut.
    - **Indiquer manuellement le nombre de processus actifs.**

Kaspersky Security for Windows Server régit le nombre de processus de travail actifs en fonction des valeurs indiquées.
    - **Quantité maximale de processus actifs**

Nombre maximum de processus utilisés par Kaspersky Security for Windows Server. Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.
    - **Nombre de processus pour la Protection en temps réel.**

Nombre maximum de processus utilisés par les composants des tâches de protection en temps réel. Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.
    - **Nombre de processus pour les tâches d'analyse à la demande en arrière-plan.**

Nombre maximum de processus utilisés par le module d'analyse à la demande quand cette analyse est réalisée en arrière-plan. Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.
  - Dans la section **Interaction avec l'utilisateur**, configurez l'affichage de l'icône de la barre d'état de l'application dans la zone de notification : décochez ou cochez la case **Afficher l'icône de la barre d'état dans la barre des tâches**.
6. Sous l'onglet **Stockage hiérarchique**, sélectionnez l'option d'accès au stockage hiérarchique (cf. section "Configuration des paramètres du système HSM via le Plug-in d'administration" à la page [546](#)).
7. Cliquez sur le bouton **OK**.

Les paramètres d'application définis seront enregistrés.

## Configuration des paramètres de sécurité dans Kaspersky Security Center

► Pour configurer les paramètres de sécurité manuellement, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Paramètres de l'application** du groupe **Sécurité**, cliquez sur le bouton **Configuration**.
5. Configurez les paramètres suivants dans la fenêtre **Paramètres de sécurité** :
  - La section **Paramètres de fiabilité** permet de configurer les paramètres de restauration des tâches de Kaspersky Security for Windows Server en cas d'échec de l'application ou d'arrêt forcé de celle-ci.
    - **Réaliser la restauration des tâches**

La case active ou désactive la restauration des tâches de Kaspersky Security for Windows Server après un échec de l'application ou un arrêt forcé de celle-ci.

Si la case est cochée, Kaspersky Security for Windows Server restaure automatiquement ses tâches après un échec de l'application ou un arrêt forcé de celle-ci.

Si la case est décochée, Kaspersky Security for Windows Server ne restaure pas ses tâches après un échec de l'application ou un arrêt forcé de celle-ci.

Cette case est cochée par défaut.
    - **Ne pas réaliser la restauration des tâches d'analyse à la demande plus de (fois)**

Nombre de tentatives de restauration des tâches d'analyse à la demande après un échec de Kaspersky Security for Windows Server. Le champ de saisie est accessible si la case **Réaliser la restauration des tâches** a été cochée.
  - La section **Action lors du passage à une source d'alimentation continue** permet de limiter la charge de Kaspersky Security for Windows Server sur le serveur dans le cadre de l'alimentation de secours :
    - **Ne pas lancer les tâches d'analyse programmée**

Cette case active ou désactive le lancement d'une tâche d'analyse programmée entre l'entrée en action de l'alimentation de secours du serveur et le rétablissement de l'alimentation normale.

Si la case est cochée, Kaspersky Security for Windows Server ne lance pas les tâches d'analyse programmée entre l'entrée en action de l'alimentation de secours du serveur et

le rétablissement de l'alimentation standard.

Si la case est décochée, Kaspersky Security for Windows Server lance les tâches d'analyse programmée quelle que soit la source d'alimentation du serveur.

Cette case est cochée par défaut.

- **Stopper les tâches d'analyse en cours**

La case active ou désactive la suspension des tâches d'analyse en cours d'exécution lors du passage du serveur à une source d'alimentation de secours.

Si la case est cochée, Kaspersky Security for Windows Server arrête l'exécution des tâches d'analyse en cours lors du passage du serveur à une source d'alimentation de secours.

Si la case est décochée, Kaspersky Security for Windows Server poursuit l'exécution des tâches d'analyse en cours après que le serveur est passé à une source d'alimentation de secours.

Cette case est cochée par défaut.

- Dans la section **Paramètres de protection par mot de passe**, définissez le mot de passe de protection de l'accès aux fonctions de Kaspersky Security for Windows Server.

6. Cliquez sur le bouton **OK**.

Les paramètres définis de sécurité et de fiabilité sont enregistrés.

## Configuration des paramètres de connexion dans Kaspersky Security Center

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Security for Windows Server et les serveurs de mise à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services KSN.

► *Pour configurer les paramètres de la connexion, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Configuration** dans le groupe

## Connexions.

La fenêtre **Paramètres de connexion** s'ouvre.

5. Configurez les paramètres suivants dans la fenêtre **Paramètres de connexion** :

- Définissez les paramètres d'utilisation du serveur proxy dans la section **Paramètres du serveur proxy** :
  - **Ne pas utiliser de serveur proxy.**

Si cette option est sélectionnée, Kaspersky Security for Windows Server n'utilise pas le serveur proxy pour la connexion aux services du KSN et effectue la connexion directement.
  - **Utiliser les paramètres du serveur proxy indiqué.**

Si cette option est sélectionnée, Kaspersky Security for Windows Server utilise les paramètres du serveur proxy indiqués manuellement pour la connexion au KSN.
  - Adresse IP ou nom symbolique du serveur proxy et numéro de port.
  - **Ne pas utiliser le serveur proxy pour les adresses locales.**

La case active ou désactive l'utilisation du serveur proxy lors des échanges avec les autres ordinateurs du réseau auquel appartient l'ordinateur disposant de Kaspersky Security for Windows Server.

Si la case est cochée, les échanges avec les autres ordinateurs du réseau auquel appartient l'ordinateur disposant de Kaspersky Security for Windows Server se font directement. Le serveur proxy n'est pas utilisé.

Si la case est décochée, les ordinateurs locaux sont sollicités via le serveur proxy.

Cette case est cochée par défaut.
- Définissez les paramètres d'authentification dans la section **Paramètres d'authentification du serveur proxy** :
  - Sélectionnez les paramètres d'authentification dans la liste déroulante.
    - **Ne pas utiliser l'authentification** : l'authentification n'est pas utilisée. Ce mode est sélectionné par défaut.
    - **Utiliser l'authentification NTLM** : authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft.
    - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** : authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft, et du nom d'utilisateur et du mot de passe.
    - **Utiliser le nom d'utilisateur et le mot de passe** : authentification à l'aide du nom d'utilisateur et du mot de passe.
  - Si nécessaire, indiquez le nom d'utilisateur et le mot de passe.
- Dans le groupe **Licence**, cochez ou décochez la case **Utiliser Kaspersky Security Center comme serveur proxy pour l'activation de l'application**.

6. Cliquez sur le bouton **OK**.

Les paramètres de la connexion définis seront enregistrés.



## Configuration du lancement planifié des tâches locales du système prédéfinies

Les stratégies permettent d'autoriser ou d'interdire le lancement des tâches locales du système d'analyse à la demande et de mise à jour programmée localement sur chaque serveur du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'ordinateur local selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.
- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Le lancement des tâches locales du système est interdit par défaut par la stratégie.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont régies via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de mise à jour de groupe ou d'analyse à la demande, autorisez le démarrage des tâches locales du système dans la stratégie : Kaspersky Security for Windows Server procède à des mises à jour des modules et des bases de données de l'application, puis démarre toutes les tâches d'analyse à la demande du système local conformément à la planification par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâches d'analyse à la demande : Analyse des zones critiques, Analyse de la quarantaine, Analyse au démarrage du système d'exploitation et Vérification de l'intégrité de l'application.
- 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.

Si vous excluez le serveur protégé du groupe d'administration, la planification des tâches système prédéfinies sera automatiquement activée.

► *Pour autoriser ou interdire le lancement planifié des tâches système de Kaspersky Security for Windows Server dans une stratégie, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Périphériques administrés**, déployez ensuite le groupe requis, puis sélectionnez l'onglet **Stratégies** dans le volet résultats.
2. Sous l'onglet **Stratégies**, ouvrez le menu contextuel de la stratégie à l'aide de laquelle vous souhaitez configurer le lancement planifié des tâches système de Kaspersky Security for Windows Server sur le groupe de serveurs et choisissez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés : <nom de la stratégie>**, ouvrez la section **Paramètres de l'application**. Cliquez sur le bouton **Lancer les tâches système** dans la section **Configuration** et réalisez les opérations suivantes :
  - Cochez les cases **Autoriser le lancement de la tâche d'analyse à la demande** et **Autoriser l'exécution des tâches de mise à jour et de copie des mises à jour** pour autoriser le lancement planifié des tâches citées.
  - Décochez les cases **Autoriser le lancement de la tâche d'analyse à la demande** et **Autoriser l'exécution des tâches de mise à jour et de copie des mises à jour** pour interdire le lancement

planifié des tâches citées.

L'activation ou la désactivation des cases n'a aucun impact sur les paramètres de lancement des tâches locales définies par l'utilisateur du type indiqué.

4. Assurez-vous que la stratégie que vous configurez est active et appliquée au groupe de serveurs sélectionné.
5. Cliquez sur le bouton **OK**.

Les paramètres définis du lancement planifié sont appliqués aux tâches sélectionnées.

## Configuration des paramètres de la quarantaine et de la Sauvegarde dans Kaspersky Security Center

► *Pour configurer les paramètres de la Sauvegarde dans Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans la sous-section **Stockages**.
5. Sous l'onglet **Sauvegarde** de la fenêtre de paramètres **Stockages**, configurez les paramètres de la Sauvegarde suivants :
  - Si vous souhaitez définir le dossier de sauvegarde, sélectionnez, dans le champ **Dossier de sauvegarde**, le dossier requis sur le disque local du serveur protégé ou saisissez le chemin d'accès complet à celui-ci.
  - Si vous souhaitez définir la taille maximale de la Sauvegarde, cochez la case **Taille maximale de sauvegarde (Mo)** et saisissez la valeur souhaitée en mégaoctets dans le champ.
  - Si vous souhaitez définir le seuil d'espace disponible dans la sauvegarde, définissez la valeur de **Taille maximale de sauvegarde (Mo)**, cochez la case **Seuil d'espace disponible (Mo)** et saisissez la valeur minimale souhaitée d'espace disponible dans la sauvegarde en mégaoctets.
  - Pour indiquer un dossier de restauration, dans la section **Paramètres de restauration**, sélectionnez le

dossier requis sur le disque local du serveur protégé ou saisissez le nom du dossier et son chemin d'accès complet dans le champ **Dossier cible pour la restauration des objets**.

6. Dans la fenêtre **Stockages**, choisissez l'onglet **Quarantaine** et configurez les paramètres de la quarantaine :
  - Si vous souhaitez modifier le dossier de la quarantaine, indiquez le chemin d'accès au dossier sur le disque local du serveur protégé dans le champ **Dossier de quarantaine**.
  - Si vous souhaitez définir la taille maximale de la quarantaine, cochez la case **Taille maximale de la quarantaine (Mo)** et saisissez la valeur en Mo dans le champ.
  - Si vous souhaitez définir la valeur minimale d'espace disponible dans la quarantaine, cochez les cases **Taille maximale de la quarantaine (Mo)** et **Seuil d'espace disponible (Mo)**, puis saisissez la valeur seuil du paramètre en Mo dans le champ de saisie.
  - Si vous souhaitez modifier le dossier dans lequel les fichiers de la quarantaine sont restaurés, saisissez le chemin d'accès complet au dossier sur le disque local du serveur à protéger dans le champ **Dossier cible pour la restauration des objets**.
7. Cliquez sur le bouton **OK**.

Les paramètres configurés de la Quarantaine et de la Sauvegarde seront enregistrés.

## Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués

Cette section décrit comment bloquer les ordinateurs bloqués et configurer les paramètres du Stockage des ordinateurs bloqués.

### Dans cette section

A propos du stockage des ordinateurs bloqués .....	<a href="#">106</a>
Configuration des paramètres de la Liste des ordinateurs bloqués .....	<a href="#">107</a>

### A propos du stockage des ordinateurs bloqués

Le Stockage des ordinateurs bloqués est installé par défaut si un des composants suivants est installé : Protection des fichiers en temps réel, Protection contre le chiffrement pour NetApp, Protection contre le chiffrement. Ces composants détectent les tentatives de chiffrement, d'ouverture ou d'exécution d'objets sur les dossiers réseau partagés du serveur protégé ou du périphérique de stockage NAS conformément à la liste des ordinateurs bloqués. Les informations relatives aux hôtes bloqués de tous les serveurs protégés sont envoyées au Kaspersky Security Center. Kaspersky Security for Windows Server bloque l'accès aux dossiers partagés ou aux dossiers de périphériques de stockage NAS pour tous les ordinateurs distants dans la liste des ordinateurs bloqués.

Le Stockage des ordinateurs bloqués est rempli quand au moins une des tâches suivantes est lancée en mode actif et quand les conditions indiquées sont remplies :

- Pour la tâche Protection des fichiers en temps réel : détection d'une activité malveillante émanant d'un ordinateur qui accède aux ressources de fichier réseau ; dans les paramètres de la tâche Protection des fichiers en temps réel, la case **Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante** est cochée.
- Pour la tâche Protection contre le chiffrement : détection d'un chiffrement malveillant réalisé par un

ordinateur qui accède aux ressources de fichier réseau.

- Pour la tâche Protection contre le chiffrement pour NetApp : détection d'une attaque contre le périphérique de stockage NAS.

Après la détection d'une activité ou d'une tentative de chiffrement malveillant, la tâche envoie les informations relatives à l'hôte à l'origine de l'attaque au stockage des ordinateurs bloqués et l'application génère un avertissement de blocage de l'hôte. Toutes les tentatives d'accès aux dossiers réseau partagés réalisées au départ de cet hôte seront bloquées.

Si l'identifiant unique local (LUID) d'un hôte à l'origine de l'attaque a été ajoutée à la liste des ordinateurs bloqués, Kaspersky Security for Windows Server détermine l'adresse IP de cet hôte et ajoute cette adresse IP à la liste des ordinateurs bloqués au lieu de l'identifiant unique local (LUID) d'un hôte à l'origine de l'attaque.

Par défaut, Kaspersky Security for Windows Server supprime les ordinateurs bloqués de la liste 30 minutes après leur ajout. L'accès de l'ordinateur aux ressources de fichier réseau est rétabli automatiquement après sa suppression de la liste des ordinateurs bloqués. Vous pouvez indiquer la durée au terme de laquelle les ordinateurs bloqués sont automatiquement débloqués.

Remarque : lorsque vous limitez l'accès pour la gestion des stockages pour n'importe quel compte utilisateur, le stockage des ordinateurs bloqués reste disponible. Les paramètres Liste des ordinateurs bloqués ne sont pas modifiables, uniquement si le compte utilisateur ne bénéficie pas des droits **Modifier les privilèges** pour l'administration de Kaspersky Security for Windows Server.

## Configuration des paramètres de la Liste des ordinateurs bloqués

► Pour configurer le stockage des ordinateurs bloqués.

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans la sous-section **Stockages**. La fenêtre **Paramètres des stockages** s'affiche.
5. Dans la section **Paramètres du blocage des hôtes** de l'onglet **Stockage de la liste des ordinateurs bloqués**, indiquez le nombre de jours, d'heures et de minutes à décompter à partir du moment du blocage

des hôtes et au terme desquels les hôtes bloqués sont de nouveau autorisés à accéder aux ressources de fichier réseau.

6. Cliquez sur le bouton **OK**.

## A propos de la configuration des journaux et notifications

La Console d'administration de Kaspersky Security Center permet de configurer les notifications adressées à l'administrateur et aux utilisateurs relatives aux événements liés à l'utilisation de Kaspersky Security for Windows Server et à l'état de la protection antivirus du serveur protégé :

- L'administrateur peut obtenir des informations sur les événements de certains types.
- les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peuvent obtenir des informations sur les événements de type *Objet détecté*.

Des notifications sur les événements Kaspersky Security for Windows Server peuvent être configurées pour un ordinateur unique via la fenêtre **Propriétés : <nom de l'ordinateur>** de l'ordinateur ou pour un groupe d'ordinateurs dans la fenêtre **Propriétés : <nom de la stratégie>** de groupe d'administration sélectionné.

L'onglet **Notifications sur les événements** ou la fenêtre **Configuration des notifications** permettent de configurer les types de notification suivants :

- L'onglet **Notifications sur les événements** (onglet standard de Kaspersky Security Center) permet de configurer les notifications adressées à l'administrateur sur les événements de certains types. Pour en savoir plus sur les modes de notification, consultez le *Système d'aide de Kaspersky Security Center*.
- La fenêtre **Configuration des notifications** permet de configurer les notifications pour l'administrateur et pour les utilisateurs.

Les notifications relatives aux événements de certains types peuvent être configurées uniquement sous l'onglet ou dans la fenêtre tandis que les notifications relatives à d'autres événements peuvent être configurées dans les deux.

Si vous configurez les notifications sur les événements d'un même type via une méthode identique sous l'onglet **Notifications sur les événements** et dans la fenêtre **Configuration des notifications**, l'administrateur système recevra les notifications relatives à ces événements via la méthode indiquée deux fois.

### Dans cette section

Configuration des paramètres du journal .....	<a href="#">109</a>
Journaux de sécurité .....	<a href="#">109</a>
Configuration des paramètres d'intégration à SIEM .....	<a href="#">110</a>
Configuration des paramètres des notifications .....	<a href="#">113</a>
Configuration de l'interaction avec le Serveur d'administration .....	<a href="#">114</a>

## Configuration des paramètres du journal

► Pour configurer les journaux de Kaspersky Security for Windows Server, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Journaux d'exécution de la tâche**.
5. Dans la fenêtre **Paramètres des journaux**, configurez les paramètres suivants de Kaspersky Security for Windows Server conformément à vos exigences :
  - Configurez le niveau de détail des événements dans les journaux. Pour ce faire, procédez comme suit :
    - a. Dans la liste **Composant**, sélectionnez le composant de Kaspersky Security for Windows Server pour lequel vous souhaitez indiquer le niveau de détails.
    - b. Pour définir le niveau de détails dans les journaux d'exécution de la tâche et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Niveau d'importance**.
  - Pour modifier l'emplacement par défaut des journaux, indiquez le chemin d'accès complet au dossier ou cliquez sur le bouton **Parcourir**.
  - Indiquez la durée de conservation en jour des journaux d'exécution des tâches.
  - Indiquez le nombre de jours pendant lesquels les informations reprises dans le nœud **Journal d'audit système** seront conservées.
6. Cliquez sur le bouton **OK**.

Les paramètres des journaux configurés sont conservés.

## Journaux de sécurité

Kaspersky Security for Windows Server tient un journal des événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le serveur protégé. Ce journal enregistre les événements suivants :

- Événements de Protection contre les exploits.
- Les événements critiques du composant Inspection des journaux.

- Les événements critiques qui indiquent une tentative de violation de la sécurité (pour les tâches Protection en temps réel du serveur, Analyse à la demande, Moniteur d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez purger les journaux de sécurité de la même manière que pour le journal d'audit système (cf. section "Suppression d'événements du journal d'audit système" à la page 216). Dans ce cas, Kaspersky Security for Windows Server enregistre l'événement d'audit système sur la purge des Journaux de sécurité.

## Configuration des paramètres d'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des volumes des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il récolte et analyse les événements reçus et réalise également d'autres actions d'administration des journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : ce mode suppose que tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'ordinateur local même après avoir été envoyés à SIEM. Il est recommandé d'utiliser ce mode pour réduire au maximum la charge sur le serveur protégé.
- Supprimer les copies locales des événements : ce mode suppose que tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans SIEM soient supprimés de l'ordinateur local.

L'application ne supprime jamais les versions locales des Journaux de sécurité.

Kaspersky Security for Windows Server peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus par le SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Pour réduire le risque d'erreur d'envoi des événements à SIEM, vous pouvez indiquer les paramètres de connexion au serveur syslog de miroir.

Le serveur syslog de miroir est un serveur syslog complémentaire vers lequel l'application passe automatiquement si la connexion au serveur principal syslog ou son utilisation sont impossibles.

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres de fonctionnement (cf. tableau ci-dessous).

Tableau 10. Paramètres d'intégration à SIEM

Paramètre	Valeur par défaut	Description
<b>Envoyer les événements à un serveur syslog externe via le protocole syslog</b>	Pas appliqué	Vous pouvez activer et désactiver l'intégration à SIEM en cochant ou décochant la case.



Paramètre	Valeur par défaut	Description
<b>Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe</b>	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi à SIEM en cochant ou décochant la case.
Format des événements	Données structurées	Vous pouvez choisir un de deux formats sous lesquels l'application convertit les événements avant de les envoyer au serveur syslog pour mieux les reconnaître au niveau du SIEM.
Protocole de connexion	TCP	Vous pouvez utiliser la liste déroulante pour configurer la connexion au serveur syslog principal via les protocoles UDP ou TCP et au serveur syslog miroir via le protocole TCP.
Paramètres de connexion au serveur syslog principal	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.
<b>Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible</b>	Pas appliqué	Vous pouvez activer et désactiver l'application du serveur syslog de miroir à l'aide de la case.
Paramètres de connexion au serveur syslog complémentaire	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog complémentaire à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.

► Pour configurer les paramètres d'intégration à SIEM, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans le groupe de paramètres **Journaux d'exécution de la tâche**.

La fenêtre **Paramètres des journaux et notifications** s'ouvre.

5. Sélectionnez l'onglet **Intégration à SIEM**.
6. Dans la section **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.

La case active ou désactive l'utilisation de la fonction d'envoi des événements publiés au serveur syslog externe.

Si la case est cochée, l'application exécute l'envoi des événements publiés sur SIEM conformément à la configuration des paramètres d'intégration à SIEM.

Si la case est décochée, l'application n'exécute pas l'intégration à SIEM. Vous ne pouvez pas configurer les paramètres d'intégration à SIEM si la case est décochée.

Cette case est décochée par défaut.

7. Si besoin, dans la section **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe**.

La case active ou désactive la suppression des copies locales des journaux au moment de leur envoi à SIEM.

Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le SIEM. Il est recommandé d'utiliser ce mode sur les ordinateurs de faible puissance.

Si la case est décochée, l'application envoie uniquement les événements à SIEM. Les copies des journaux continuent d'être conservées localement.

Cette case est décochée par défaut.

L'état de la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe** n'influence pas les paramètres de conservation des événements des Journaux de sécurité : l'application ne supprime jamais automatiquement les événements des Journaux de sécurité.

8. Dans la section **Format des événements**, indiquez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi à SIEM.

Par défaut, l'application exécute la conversion au format de données structurées.

9. Dans la section **Paramètres de connexion**, procédez comme suit :

- Indiquez le protocole de connexion à SIEM.
- Indiquez les paramètres de connexion au serveur syslog principal.  
Vous pouvez indiquer l'adresse IP uniquement au format IPv4.
- Cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si vous voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n'est pas possible.

- Définissez les paramètres suivants de connexion au serveur syslog de miroir : **Adresse IP** et **Port**.

Les champs **Adresse IP** et **Port** pour le serveur syslog de miroir ne peuvent pas être modifiés si la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible** est décochée.

Vous pouvez indiquer l'adresse IP uniquement au format IPv4.

10. Cliquez sur le bouton **OK**.

Les paramètres d'intégration à SIEM configurés seront appliqués.

## Configuration des paramètres des notifications

► *Pour configurer les notifications de Kaspersky Security for Windows Server, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans la sous-section **Notifications sur les événements**.
5. Dans la fenêtre **Configuration des notifications**, configurez les paramètres suivants de Kaspersky Security for Windows Server conformément à vos exigences :
  - Sélectionnez le type de notification dont vous souhaitez configurer les paramètres dans la liste **Configuration des notifications**.
  - Configurez le mode de notification de l'utilisateur dans la section **Informez les utilisateurs**. Le cas échéant, rédigez le texte de la notification.
  - Configurez le mode de notification de l'administration dans la section **Informez les administrateurs**. Le cas échéant, rédigez le texte de la notification. Le cas échéant, cliquez sur **Configuration** pour configurer les paramètres supplémentaires des notifications.
  - Définissez dans la section **Seuils de déclenchement des événements** les intervalles à l'issue desquels Kaspersky Security for Windows Server enregistre les événements *Bases de l'application dépassées*, *Bases de l'application fortement dépassées* et *Analyse rapide non réalisée depuis longtemps*.

- **Bases de l'application dépassées (jours)**  
Nombre de jours écoulés depuis la dernière mise à jour des bases de l'application.  
La valeur par défaut est de 7 jours.
- **Bases de l'application fortement dépassées (jours)**  
Nombre de jours écoulés depuis la dernière mise à jour des bases de l'application.  
La valeur par défaut est de 14 jours.
- **Analyse des zones critiques non réalisée depuis longtemps (jours)**  
Nombre de jours depuis la dernière exécution réussie de la tâche d'analyse rapide.  
La valeur par défaut est de 30 jours.

6. Cliquez sur le bouton **OK**.

Les paramètres de la notification définis seront enregistrés.

## Configuration de l'interaction avec le Serveur d'administration

► *Pour sélectionner les types des objets au sujet desquels Kaspersky Security for Windows Server va envoyer des informations au serveur d'administration de Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Cliquez sur le bouton **Configuration** dans le bloc **Interaction avec le Serveur d'administration** de la section **Journaux et notifications**.

La fenêtre **Listes réseau du Serveur d'administration** s'ouvre.

5. Dans la fenêtre **Listes réseau du Serveur d'administration**, choisissez les types d'objets au sujet desquels Kaspersky Security for Windows Server va transmettre des informations au serveur d'administration de Kaspersky Security Center :

- Objets en quarantaine.
  - Objets sauvegardés.
  - Liste des ordinateurs bloqués.
6. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server transmet les informations relatives aux types d'objets choisis au Serveur d'administration.

## Création et configuration des stratégies



Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Security for Windows Server sur plusieurs serveurs.



Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs serveurs sur lesquels Kaspersky Security for Windows Server est installé.


Une stratégie applique les paramètres de Kaspersky Security for Windows Server, de ses fonctions et de ses tâches à l'ensemble des serveurs protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la Console d'administration, la stratégie active dans le groupe en ce moment possède l'état *actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Security for Windows Server. Vous pouvez les consulter dans la console de l'application dans le nœud **Journal d'audit système**.

Il existe dans Kaspersky Security Center une méthode unique pour appliquer des stratégies aux ordinateurs locaux : *Interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Security for Windows Server applique aux ordinateurs locaux les valeurs des paramètres en regard desquels vous avez sélectionné l'icône  dans les propriétés de la stratégie au lieu de la valeur des paramètres en vigueur avant l'application de la stratégie. Les paramètres de la stratégie active accompagnés de l'icône  dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Security for Windows Server.

Si une stratégie est active, les paramètres dans la console de l'application qui sont accompagnés de l'icône  dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres (accompagnés de l'icône  dans la stratégie) peuvent être modifiées dans la console de l'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône  empêchent également la modification des paramètres dans Kaspersky Security Center pour un ordinateur depuis la fenêtre

**Propriétés <Nom de l'ordinateur> :**

Les paramètres configurés et transmis à l'ordinateur local à l'aide de la stratégie active sont enregistrés dans les paramètres des tâches locales après la désactivation de la stratégie active.

Si la stratégie définit les paramètres d'une tâche de protection en temps réel ou de protection des stockages réseau, et si cette tâche est en exécution, les paramètres définis par la stratégie sont modifiés directement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

### Contenu du chapitre

Création d'une stratégie.....	<a href="#">117</a>
Sections contenant les paramètres de stratégie de Kaspersky Security for Windows Server.....	<a href="#">119</a>
Configuration de stratégie.....	<a href="#">123</a>

## Création d'une stratégie

La création d'une stratégie comporte les étapes suivantes :


1. Création d'une stratégie à l'aide de l'Assistant de création de stratégies. Vous pouvez définir les paramètres des tâches Protection en temps réel du serveur dans les boîtes de dialogue de l'assistant.
  2. Configuration des paramètres de la stratégie. La fenêtre **Propriétés : <Nom de la stratégie>** de la stratégie créée permet de configurer les paramètres des tâches Protection en temps réel du serveur, les paramètres généraux de Kaspersky Security for Windows Server, les paramètres de la quarantaine et les paramètres de la Sauvegarde, le niveau de détail des journaux d'exécution de la tâche ainsi que les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Security for Windows Server.
- *Pour créer une stratégie pour un groupe de serveurs sur lesquels Kaspersky Security for Windows Server est installé, procédez comme suit :*

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, déployez le nœud **Périphériques administrés**, puis sélectionnez le groupe d'administration contenant les serveurs pour lesquels vous souhaitez créer une stratégie.
2. Dans le panneau de détails du groupe d'administration sélectionné, choisissez l'onglet **Stratégies** et cliquez sur le lien **Créer une stratégie** pour démarrer l'assistant et créer une stratégie.

La fenêtre **Assistant de création de stratégie** s'ouvre.


3. Dans la fenêtre **Sélection de l'application pour la création d'une stratégie de groupe**, choisissez Kaspersky Security for Windows Server et cliquez sur **Suivant**.
4. Entrez un nom de stratégie de groupe dans le champ **Nom**.

Le nom de la stratégie ne peut pas contenir les caractères suivants : " \* < : > ? \ | .

5. Pour appliquer la configuration de stratégie utilisée pour l'application précédente, procédez comme suit :
  - a. Cochez la case **Utiliser les paramètres de la stratégie pour les versions précédentes de l'application**.
  - b. Cliquez sur le bouton **Sélectionner**.
  - c. Sélectionnez la stratégie que vous souhaitez appliquer.
  - d. Cliquez sur **Suivant**.
6. Sélectionnez une des options suivantes dans la fenêtre **Sélection du type d'opération** :
  - **Nouveau** pour créer une stratégie avec les paramètres par défaut.
  - **Importer une stratégie créée avec des versions antérieures de Kaspersky Security for Windows Server** pour utiliser la stratégie de cette version en tant que modèle.
  - Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de configuration dans lequel vous avez enregistré la stratégie existante.
7. Dans la fenêtre **Protection en temps réel du serveur**, configurez les tâches Protection des fichiers en temps réel, Utilisation du KSN, la fonctionnalité Protection contre les exploits et la fonctionnalité Monitoring des scripts en fonction de vos besoins. Autorisez ou interdisez l'application des tâches configurées de la stratégie sur les ordinateurs locaux du réseau :
  - Cliquez sur le bouton  pour débloquer la configuration des paramètres d'une tâche sur les ordinateurs



du réseau et interdire l'application des paramètres de la tâche configurés dans la stratégie.

- Cliquez sur le bouton  pour interdire la configuration des paramètres d'une tâche sur les ordinateurs du réseau et autoriser l'application des paramètres de la tâche configurés dans la stratégie.

Dans une stratégie recréée, les paramètres des tâches de protection en temps réel du serveur sont définis par défaut.

- Si vous souhaitez modifier les paramètres d'une tâche Protection des fichiers en temps réel définis par défaut, cliquez sur le bouton **Configuration** dans la sous-section **Protection des fichiers en temps réel**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos exigences. Cliquez sur le bouton **OK**.
- Si vous souhaitez modifier les paramètres d'une tâche Utilisation du KSN définis par défaut, cliquez sur le bouton **Configuration** dans la sous-section **Utilisation du KSN**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos exigences. Cliquez sur le bouton **OK**.

Pour démarrer la tâche Utilisation du KSN, vous devez accepter la déclaration KSN dans la fenêtre **Traitement des données** (cf. section "Configuration du traitement des données via le Plug-in d'administration" à la page [299](#)).

- Pour modifier les paramètres par défaut du composant Protection contre les exploits, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre les exploits**. Dans la fenêtre qui s'ouvre, configurez la fonctionnalité en fonction de vos exigences. Cliquez sur le bouton **OK**.
8. Sélectionnez un des états suivants de la stratégie suivants dans la fenêtre **Créer la stratégie de groupe pour l'application** :
- **Stratégie active** si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, celle-ci est désactivée et une nouvelle stratégie est appliquée.
  - **Stratégie inactive**, si vous ne voulez pas appliquer immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.
  - Cochez la case **Ouvrir les propriétés de la stratégie uniquement après leur création** pour fermer automatiquement l'**assistant de création de stratégie** et configurez la stratégie récemment créée après avoir cliqué sur le bouton **Suivant**.
9. Cliquez sur le bouton **Terminer**.

La stratégie créée sera affichée dans la liste des stratégies sous l'onglet **Stratégies** du groupe d'administration sélectionné. La fenêtre **Propriétés : <nom de la stratégie>** permet de configurer d'autres paramètres, tâches et fonctions de Kaspersky Security for Windows Server.

## Sections contenant les paramètres de stratégie de Kaspersky Security for Windows Server

### Général

La section **Général** permet de configurer les paramètres de stratégie suivants :

- Indiquez l'état de la stratégie.
- Héritage des paramètres des stratégies parent pour les stratégies fille.

### Configuration d'événement

La section **Configuration d'événement** permet de configurer les paramètres pour les catégories d'événements suivants :

- *Evénements critiques*
- *Panne de fonction*
- *Avertissement*
- *Message d'information*

Le bouton **Propriétés** permet de configurer les paramètres suivants pour les événements sélectionnés :

- Définir l'emplacement et la durée de conservation des informations sur l'événement enregistré ;
- Sélection du mode de notification sur les événements enregistrés.

### Paramètres de l'application

Tableau 11. Paramètres de la section Paramètres de l'application

Section	Options
<b>Montée en puissance et interface</b>	Le bouton <b>Configuration</b> de la sous-section <b>Montée en puissance et interface</b> permet de configurer les paramètres suivants : <ul style="list-style-type: none"> <li>• choisir la configuration automatique ou manuelle des paramètres de montée en puissance ;</li> <li>• configurer l'affichage de l'icône de l'application.</li> </ul>
<b>Sécurité</b>	Le bouton <b>Configuration</b> de la sous-section <b>Sécurité</b> permet de configurer les paramètres suivants : <ul style="list-style-type: none"> <li>• Configurez les paramètres de lancement de la tâche.</li> <li>• Actions de l'application en cas de passage à l'alimentation du serveur via un onduleur.</li> <li>• Activation ou désactivation de la protection par mot de passe des fonctions de l'application.</li> </ul>
<b>Connexions</b>	Le bouton <b>Configuration</b> de la sous-section <b>Connexions</b> permet de configurer les paramètres suivants du serveur proxy pour la connexion aux serveurs de mise à jour, aux serveurs d'activation et à KSN : <ul style="list-style-type: none"> <li>• définition des paramètres du serveur proxy ;</li> <li>• définition des paramètres d'authentification sur le serveur proxy.</li> </ul>
<b>Lancer les tâches système</b>	Le bouton <b>Configuration</b> de la sous-section <b>Lancer les tâches système</b> permet d'interdire ou d'autoriser le lancement des tâches système planifiées suivantes, configurées sur les ordinateurs locaux : <ul style="list-style-type: none"> <li>• Tâche Analyse à la demande.</li> <li>• Tâches de mise à jour et de copie des mises à jour.</li> </ul>

## Complémentaire

Tableau 12. Paramètres de la section Complémentaire

Section	Options
<b>Zone de confiance</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Zone de confiance</b> permet de configurer les paramètres suivants d'application d'une zone de confiance :</p> <ul style="list-style-type: none"> <li>• Composer la liste des exclusions de la zone de confiance.</li> <li>• Activer ou désactiver l'analyse des opérations de sauvegarde des fichiers.</li> <li>• Composer une liste des processus de confiance.</li> </ul>
<b>Analyse des disques amovibles</b>	<p>La section <b>Analyse des disques amovibles</b> contient le bouton <b>Configuration</b> qui permet de configurer les paramètres d'analyse des disques USB amovibles.</p>
<b>Autorisations d'accès de l'utilisateur pour l'administration de l'application</b>	<p>La sous-section <b>Autorisations d'accès de l'utilisateur pour l'administration de l'application</b> permet de configurer les paramètres des droits des utilisateurs et des groupes d'utilisateurs à l'administration de Kaspersky Security for Windows Server.</p>
<b>Autorisations d'accès de l'utilisateur pour l'administration du service Security</b>	<p>La sous-section <b>Autorisations d'accès de l'utilisateur pour l'administration du service Security</b> permet de configurer les droits des utilisateurs et des groupes d'utilisateurs à l'administration du service Kaspersky Security.</p>
<b>Stockages</b>	<p>Dans la sous-section <b>Stockages</b>, cliquez sur le bouton <b>Configuration</b> pour configurer les paramètres suivants de la quarantaine, de la Sauvegarde et de la liste des ordinateurs bloqués :</p> <ul style="list-style-type: none"> <li>• chemin d'accès du dossier dans lequel vous souhaitez placer les objets en quarantaine ou dans la sauvegarde ;</li> <li>• taille maximale de la Sauvegarde ou de la quarantaine et seuil d'espace disponible ;</li> <li>• dossier où seront placés les objets restaurés depuis la sauvegarde ou la quarantaine ;</li> <li>• configurez les paramètres du blocage des hôtes.</li> </ul>

## Protection en temps réel du serveur

Tableau 13. Paramètres de la section Protection en temps réel du serveur

Section	Options
<b>Protection des fichiers en temps réel</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Protection des fichiers en temps réel</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• Indiquez le mode de protection.</li> <li>• Configurez l'utilisation de l'analyse heuristique.</li> <li>• Configurez l'application de la Zone de confiance.</li> <li>• Composition de la zone de protection.</li> <li>• Niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de sécurité.</li> <li>• Configurez les paramètres de lancement de la tâche.</li> </ul>

<b>Utilisation du KSN</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Utilisation du KSN</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• actions à réaliser sur les objets considérés comme douteux par KSN ;</li> <li>• configurez le transfert de données et l'utilisation de Kaspersky Security Center en tant que serveur proxy du KSN.</li> </ul> <p>Cliquez sur le bouton <b>Traitement des données</b> pour accepter ou rejeter la Déclaration de KSN et la Déclaration de KMP, puis configurez les paramètres d'échange de données fiables.</p>
<b>Protection contre les exploits</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Protection contre les exploits</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• sélection du mode de protection de la mémoire des processus ;</li> <li>• définition de l'action de réduction de l'impact de l'exploitation des vulnérabilités ;</li> <li>• enrichissement et modification de la liste des processus à protéger.</li> </ul>

### Contrôle de l'activité locale

Tableau 14. Paramètres de la section Contrôle de l'activité locale

Section	Options
<b>Contrôle du lancement des applications</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Contrôle du lancement des applications</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• Sélectionnez le mode de fonctionnement de la tâche.</li> <li>• Configuration des paramètres du contrôle du nouveau lancement des applications.</li> <li>• Indiquez la zone d'application des règles du contrôle du lancement des applications.</li> <li>• Configuration de l'utilisation du KSN.</li> <li>• Configurez les paramètres de lancement de la tâche.</li> </ul>
<b>Contrôle des périphériques</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Contrôle des périphériques</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• Sélectionnez le mode de fonctionnement de la tâche.</li> <li>• Configurez les paramètres de lancement de la tâche.</li> </ul>

### Contrôle de l'activité réseau

Tableau 15. Paramètres de la section Contrôle de l'activité réseau

Section	Options
<b>Gestion du pare-feu</b>	<p>Le bouton <b>Configuration</b> de la sous-section <b>Gestion du pare-feu</b> permet de configurer les paramètres suivants d'exécution de la tâche :</p> <ul style="list-style-type: none"> <li>• Règles du pare-feu.</li> <li>• Configurez les paramètres de lancement de la tâche.</li> </ul>

### Diagnostic du système

Tableau 16. Paramètres de la section Diagnostic du système

Section	Options
<b>Moniteur d'intégrité des fichiers</b>	La sous-section <b>Moniteur d'intégrité des fichiers</b> permet de configurer le contrôle sur les modifications dans les fichiers qui peuvent indiquer un cas d'atteinte à la sécurité sur un serveur protégé.
<b>Inspection des journaux</b>	La section <b>Inspection des journaux</b> permet de configurer le contrôle de l'intégrité d'un serveur protégé sur la base des résultats de l'analyse du journal des événements Windows.

## Journaux et notifications

Tableau 17. Paramètres de la section Journaux et notifications

Section	Options
<b>Journaux d'exécution de la tâche</b>	Le bouton <b>Configuration</b> de la sous-section <b>Journaux d'exécution de la tâche</b> permet de configurer les paramètres suivants : <ul style="list-style-type: none"> <li>• Définition du niveau d'importance des événements enregistrés pour les composants de l'application sélectionnés ;</li> <li>• Définition des paramètres de conservation des journaux d'exécution de la tâche.</li> <li>• Spécifiez l'intégration de SIEM avec les paramètres de Kaspersky Security Center.</li> </ul>
<b>Notifications sur les événements</b>	Le bouton <b>Configuration</b> de la sous-section <b>Notifications sur les événements</b> permet de configurer les paramètres suivants : <ul style="list-style-type: none"> <li>• Définissez les paramètres de notification des utilisateurs pour l'événement <i>Objet détecté</i> ; pour les événements <i>Objet détecté</i>, <i>Stockage de masse douteux détecté et restreint</i> et <i>Hôte ajouté à la liste des ordinateurs bloqués</i>.</li> <li>• Paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements de la section <b>Configuration des notifications</b>.</li> </ul>
<b>Interaction avec le Serveur d'administration</b>	Le bouton <b>Configuration</b> de la section <b>Interaction avec le Serveur d'administration</b> permet de choisir les types d'objets que Kaspersky Security for Windows Server va signaler au Serveur d'administration. Vous pouvez également configurer la transmission au Serveur d'administration des informations relatives aux objets dans la sauvegarde ou la quarantaine.

Pour en savoir plus sur les tâches Protection des stockages réseau, consultez le [Manuel d'implantation pour la Protection des stockages réseau de Kaspersky Security for Windows Server](#).

## Historique des révisions

La section **Historique des révisions** permet d'administrer les révisions : comparer à la révision actuelle ou à une autre stratégie, ajouter des descriptions de révisions, enregistrer les révisions dans un fichier ou revenir à l'état antérieur à la révision.

## Configuration de stratégie

La fenêtre **Propriétés : <Nom de la stratégie>** d'une stratégie existante permet de configurer les paramètres généraux de Kaspersky Security for Windows Server, les paramètres de la quarantaine et de la Sauvegarde, les paramètres de la zone de confiance, les paramètres de la Protection en temps réel du serveur, les paramètres du Contrôle de l'activité locale, le niveau de détail des journaux d'exécution de la tâche, les notifications des utilisateurs et des administrateurs relatives aux événements de Kaspersky Security for Windows Server, les privilèges d'accès à l'administration de l'application et du service Kaspersky Security et les paramètres d'application des profils de stratégie.

► *Pour configurer les paramètres d'une stratégie, procédez comme suit :*

1. Développez le nœud **Périphériques administrés** dans l'arborescence de la Console d'administration de Kaspersky Security Center.
2. Développez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de la stratégie associée et ouvrez l'onglet **Stratégies** dans le panneau de détails.
3. Sélectionnez une stratégie à configurer et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** à l'aide d'une des méthodes suivantes :
  - Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.
  - Dans le panneau de droite des détails de l'entrée sélectionnée, cliquez sur le lien **Configurer la stratégie**.
  - Double-cliquez sur la stratégie sélectionnée.
4. Activez ou désactivez l'application de la stratégie dans la section **Etat de la stratégie** de l'onglet **Général**. Pour ce faire, sélectionnez l'une des options suivantes :
  - **Stratégie active** si vous souhaitez que la stratégie s'applique à tous les services appartenant au groupe d'administration sélectionné.
  - **Stratégie inactive** si vous souhaitez activer la stratégie plus tard sur tous les serveurs appartenant au groupe d'administration sélectionné.

Le paramètre **Stratégie hors du bureau** n'est pas disponible dans le cadre de la gestion de Kaspersky Security for Windows Server.

5. Dans les sections **Notifications sur les événements**, **Paramètres de l'application**, **Complémentaire**, **Journaux et notifications** et **Historique des révisions**, vous pouvez modifier la configuration de l'application (cf. tableau ci-dessous).
6. Dans les sections **Protection en temps réel du serveur**, **Contrôle de l'activité locale**, **Contrôle de l'activité réseau** et **Diagnostic du système**, configurez les paramètres de l'application et de leur lancement (cf. tableau ci-dessous).

Vous pouvez activer ou désactiver l'exécution de n'importe quelle tâche sur tous les serveurs appartenant au groupe d'administration à l'aide d'une stratégie de Kaspersky Security Center. Vous pouvez configurer l'application des paramètres définis dans la stratégie sur tous les ordinateurs du réseau pour chaque composant distinct de l'application.

7. Cliquez sur le bouton **OK**.

Les paramètres définis seront appliqués dans la stratégie.

# Création et configuration de tâches via Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Security for Windows Server, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

## Contenu du chapitre

A propos de la création de tâches dans Kaspersky Security Center .....	<a href="#">124</a>
Création d'une tâche dans Kaspersky Security Center .....	<a href="#">125</a>
Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center .....	<a href="#">127</a>
Configuration des tâches de groupe dans Kaspersky Security Center .....	<a href="#">128</a>
Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center .....	<a href="#">136</a>
Programmation des tâches .....	<a href="#">138</a>

## A propos de la création de tâches dans Kaspersky Security Center

Vous pouvez créer des tâches de groupe pour des groupes d'administration et pour des sélections d'ordinateurs. Vous pouvez créer les types de tâche suivants :

- Activation de l'application ;
- Copie des mises à jour ;
- Mise à jour des bases de l'application ;
- Mise à jour des modules de l'application ;
- Annulation de la mise à jour des bases de l'application ;
- Analyse à la demande ;
- Vérification de l'intégrité de l'application ;
- Génération des règles du Contrôle du lancement des applications ;
- Génération des règles du Contrôle des périphériques.

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- Pour un ordinateur : dans la fenêtre **Propriétés <nom de l'ordinateur>** dans la section **Tâches**.
- Pour un groupe d'administration : dans le panneau de détails du nœud du groupe d'ordinateurs sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'ordinateurs : dans le panneau de détails du nœud **Sélection de périphériques**.



Les stratégies permettent de désactiver les planifications pour les tâches locales du système de mise à jour et d'analyse à la demande (cf. section "Configuration du lancement planifié des tâches locales du système prédéfinies" à la page [104](#)) sur tous les serveurs protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

## Création d'une tâche dans Kaspersky Security Center

► Pour créer une tâche dans la console d'administration de Kaspersky Security Center, procédez comme suit :

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :
  - Pour créer une tâche locale :
    - a. Dans l'arborescence de la Console d'administration, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
    - b. Dans le panneau de détails, sous l'onglet **Périphériques**, ouvrez le menu contextuel de la ligne du serveur protégé et sélectionnez **Propriétés**.
    - c. Dans la section **Tâches** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
  - Pour créer une tâche de groupe :
    - a. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
    - b. Sélectionnez le groupe d'administration pour lequel vous souhaitez créer une tâche.
    - c. Dans le panneau de détails, ouvrez l'onglet **Tâches** et choisissez l'option **Créer une tâche**.
  - Pour créer une tâche pour une sélection personnalisée de serveurs, dans le nœud **Sélections de périphériques** dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez un appareil, puis dans la liste déroulante **Exécuter une action**, sélectionnez l'option **Créer une tâche** pour l'appareil concerné.

La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la fenêtre **Sélectionnez le type de tâche**, sous le titre **Kaspersky Security for Windows Server**, sélectionnez le type de la tâche à créer.
3. Si vous avez choisi n'importe quel type de tâche, sauf Annulation de la mise à jour des bases de l'application, Vérification de l'intégrité de l'application ou Activation de l'application, la fenêtre **Configuration** s'ouvre. Les paramètres peuvent varier en fonction du type de tâche :
  - Créez une tâche d'analyse à la demande (cf. section "Création d'une tâche d'analyse à la demande" à la page [488](#)).
  - Si vous créez une des tâches de mise à jour, définissez les paramètres de la tâche conformément à vos exigences :
    - a. Sélectionnez la source des mises à jour dans la fenêtre **Source des mises à jour**.
    - b. Cliquez sur le bouton **Paramètres de connexion**. La fenêtre **Paramètres de connexion** s'ouvre.
    - c. A la fenêtre **Paramètres de connexion** :

Désignez le mode du serveur FTP pour la connexion au serveur protégé.

Le cas échéant, modifiez le délai d'attente pour la connexion au serveur de mise à jour.

Configurez les paramètres d'accès au serveur proxy lors de la connexion à la source des mises à jour.

Indiquez l'emplacement du serveur protégé (ou des serveurs) pour optimiser la récupération des mises à jour.

- Pour créer 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 **Paramètres de mise à jour des modules de l'application** :
  - a. Décidez si vous souhaitez copier et installer les mises à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles sans installation.
  - b. Si vous avez choisi **Copier et installer les mises à jour critiques des modules de l'application**, le redémarrage du serveur peut être requis pour terminer l'installation des modules de l'application. Pour que Kaspersky Security for Windows Server relance automatiquement le serveur après la fin de la tâche, cochez la case **Autoriser le redémarrage du système d'exploitation**.
  - c. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour des modules de Kaspersky Security for Windows Server, 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 mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Il est possible de configurer une notification pour l'administrateur au sujet de l'événement **Nouvelle mise à jour prévue des modules de l'application disponible**. Cette notification reprend l'adresse Internet de notre site depuis lequel il est possible de télécharger les mises à jour planifiées.

- Pour créer la tâche Copie des mises à jour, indiquez, dans la fenêtre **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.
  - Pour créer la tâche d'Activation de l'application, procédez comme suit :
    - a. Dans la fenêtre **Paramètres d'activation**, appliquez le fichier clé ou le code d'activation à l'aide duquel vous souhaitez activer l'application.
    - b. Cochez la case **Utiliser en tant que clé supplémentaire** si vous souhaitez créer une tâche pour renouveler la licence.
  - Créez la tâche Génération des règles du Contrôle du lancement des applications (cf. section "Création d'une tâche Génération des règles du Contrôle du lancement des applications" à la page [390](#)).
  - Créez la tâche Génération des règles du Contrôle des périphériques (cf. section "Création de règles à l'aide de la tâche Génération des règles du Contrôle des périphériques" à la page [431](#)).
4. Configurez la planification de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [138](#)) (vous pouvez configurer une planification pour tous les types de tâche, sauf la tâche Annulation de la mise à jour des bases de l'application).
  5. Cliquez sur le bouton **OK**.
  6. Si la tâche est créée pour une sélection quelconque de serveurs, sélectionnez le réseau (ou le groupe) de serveurs sur lesquels elle sera exécutée.
  7. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte sous les autorisations duquel vous souhaitez exécuter la tâche.
  8. Dans la fenêtre **Définition du nom de la tâche**, saisissez le nom de la tâche (100 caractères maximum) qui

ne peut pas contenir les caractères " \* < > ? \ | :.

Il est conseillé d'indiquer le type de tâche dans son nom (par exemple, Analyse à la demande du dossier partagé).

9. Dans la fenêtre **Fin de la création de la tâche**, cochez la case **Lancer la tâche à la fin de l'Assistant** si vous souhaitez que la tâche soit lancée après sa création. Cliquez sur le bouton **Terminer**.

La tâche créée apparaît dans la liste **Tâches**.

## Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center

► *Pour configurer les tâches locales ou les paramètres généraux de l'application pour un seul serveur du réseau, ouvrez la fenêtre **Paramètres de l'application** et procédez comme suit :*

1. Dans l'arborescence du Serveur d'administration de Kaspersky Security Center, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.
2. Dans le panneau de détails, choisissez l'onglet **Périphériques**.
3. Ouvrez la fenêtre **Propriétés : <Nom de l'ordinateur>** à l'aide d'une des méthodes suivantes :
  - Double-clic sur le nom du serveur protégé.
  - Ouvrez le menu contextuel du nom du serveur protégé et sélectionnez l'option **Propriétés**.

La fenêtre **Propriétés : <Nom de l'ordinateur>** s'ouvre.

4. Pour configurer les paramètres de la tâche locale, procédez comme suit :
  - a. Passez à la section **Tâches**.
    - Dans la liste des tâches, sélectionnez la tâche locale dont vous souhaitez configurer les paramètres.
    - Double-cliquez sur le nom de la tâche dans la liste des tâches.
    - Sélectionnez le nom de la tâche et cliquez sur le bouton **Propriétés**.
    - Puis, choisissez l'option **Propriétés** dans le menu contextuel de la tâche choisie.
5. Pour configurer les paramètres de l'application, procédez comme suit :
  - a. Passez à la section **Applications**.
    - Dans la liste des applications installées, sélectionnez une application à configurer.
    - Double-cliquez sur le nom de l'application dans la liste des applications installées.
    - Sélectionnez le nom de l'application dans la liste, puis cliquez sur le bouton **Propriétés**.
    - Ouvrez le menu contextuel du nom de l'application dans la liste des applications installées, puis choisissez l'option **Propriétés**.

Si l'application est soumise à une stratégie de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne pourront pas être modifiés via la fenêtre **Paramètres de l'application**.

## Configuration des tâches de groupe dans Kaspersky Security Center

► Pour configurer une tâche de groupe pour plusieurs serveurs, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
  - Double-cliquez sur le nom de la tâche dans la liste des tâches créées ;
  - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche**.
  - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.
4. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

5. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
  - Si vous configurez une tâche d'analyse à la demande :
    - a. Dans la section **Zone d'analyse**, créez une zone d'analyse.
    - b. Dans la section **Options**, configurez l'intégration aux autres modules de l'application et le niveau de priorité de la tâche.
  - Si vous configurez l'une des tâches de mise à jour, définissez les paramètres de la tâche en fonction de vos besoins :
    - a. Dans la section **Configuration**, configurez les paramètres de la source des mises à jour et l'optimisation de l'utilisation du sous-système disque.
    - b. Cliquez sur le bouton **Paramètres de connexion** pour configurer les paramètres de connexion de la source des mises à jour.
  - Pour configurer la tâche Mise à jour des modules de l'application, sélectionnez dans la section **Paramètres de mise à jour des modules de l'application** une action à effectuer : copier et installer les mises à jour critiques des modules de l'application ou simplement les rechercher.
  - Pour configurer la tâche Copie des mises à jour, indiquez, dans la section **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.
  - Pour configurer la tâche Activation de l'application, appliquez le fichier clé ou le code d'activation à l'aide duquel vous souhaitez activer l'application dans la section **Paramètres d'activation**. Cochez la case **Utiliser en tant que clé supplémentaire** si vous souhaitez ajouter un code d'activation ou un fichier clé pour renouveler la licence.
  - Si vous configurez une des tâches de création automatique des règles d'autorisation du contrôle du serveur, désignez dans la section **Configuration** les paramètres qui vont servir de base à la création de la règle d'autorisation.

6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.
8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.
9. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

Les paramètres des tâches de groupe pouvant être configurés sont décrits dans le tableau ci-dessous.

Tableau 18. Paramètre de tâches de groupe de Kaspersky Security for Windows Server

Types de tâche de Kaspersky Security for Windows Server	Section dans la fenêtre Propriétés : <nom de la tâche>	Paramètres de la tâche
Génération des règles du Contrôle du lancement des applications	<b>Configuration</b>	Lors de la configuration des paramètres de la tâche Génération des règles du Contrôle du lancement des applications, vous pouvez : <ul style="list-style-type: none"> <li>• Créer des règles d'autorisation sur la base des applications en cours d'exécution ;</li> <li>• Créer des règles d'autorisation pour les applications de dossiers spécifiques.</li> </ul>
	<b>Options</b>	Vous pouvez indiquer les actions lors de la création des règles d'autorisation du contrôle du lancement des applications : <ul style="list-style-type: none"> <li>• <b>Utiliser un certificat numérique</b></li> <li>• <b>Utiliser l'objet et l'empreinte du certificat numérique</b></li> <li>• <b>En cas d'absence de certificat, utiliser</b></li> <li>• <b>Utiliser le hash SHA256</b></li> <li>• <b>Créer des règles pour un utilisateur ou un groupe d'utilisateurs</b></li> </ul> Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security for Windows Server crée à la fin des tâches.
	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Génération des règles du Contrôle des périphériques	<b>Configuration</b>	<ul style="list-style-type: none"> <li>• sélectionnez le mode de fonctionnement :tenir compte des données système relatives à tous les périphériques de stockage de masse jamais connectés ou tenir compte uniquement des périphériques de stockage de masse connecté actuellement.</li> <li>• Configurez les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security for Windows Server crée à la fin des tâches.</li> </ul>
	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Activation de l'application (cf. section "Tâche Activation de l'application" à la page <a href="#">133</a> ).	<b>Paramètres d'activation</b>	Vous pouvez ajouter un code d'activation ou un fichier clé pour l'activation de l'application ou le renouvellement la licence.
	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Copie des mises à jour (cf. section "Tâches de mise à jour" à la page <a href="#">133</a> ).	<b>Source des mises à jour</b>	<p>Vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky Lab en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.</p> <p>Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs personnalisés manuellement.</p>
	<b>Fenêtre Paramètres de connexion</b>	Dans la fenêtre <b>Paramètres de connexion</b> ouverte depuis la section <b>Source des mises à jour</b> , indiquez s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.
	<b>Paramètres de copie des mises à jour</b>	<p>Vous pouvez indiquer le contenu des mises à jour à copier.</p> <p>Dans le champ <b>Dossier de conservation locale des mises à jour copiées</b>, indiquez le chemin d'accès au dossier dans lequel Kaspersky Security for Windows Server va conserver les mises à jour copiées.</p>
	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

<p>Mise à jour des bases de l'application (cf. section "Tâche de mise à jour" à la page <a href="#">133</a>).</p>	<p><b>Configuration</b></p>	<p>Dans la zone de groupe <b>Source des mises à jour</b>, vous pouvez indiquer le serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.</p> <p>Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs personnalisés manuellement.</p> <p>La section Optimisation de l'utilisation du sous-système de disque vous permet de configurer les paramètres de la fonction de réduction de la charge sur le sous-système disque :</p> <ul style="list-style-type: none"> <li>• <b>Réduire la charge sur les I/O du disque</b></li> <li>• <b>Volume de mémoire vive utilisé pour l'optimisation (en Mo)</b></li> </ul>
	<p>Fenêtre <b>Paramètres de connexion</b></p>	<p>Dans la fenêtre <b>Paramètres de connexion</b> ouverte depuis la section <b>Source des mises à jour</b>, indiquez s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.</p>
	<p><b>Planification</b></p>	<p>Vous pouvez configurer les paramètres de lancement de la tâche planifiée.</p>
<p>Mise à jour des modules de l'application (cf. section "Tâche de mise à jour" à la page <a href="#">133</a>).</p>	<p><b>Source des mises à jour</b></p>	<p>Vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky Lab en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.</p> <p>Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs personnalisés manuellement.</p>
	<p>Fenêtre <b>Paramètres de connexion</b></p>	<p>La zone de groupe <b>Paramètres de connexion à la source des mises à jour</b> permet d'indiquer s'il faut établir la connexion aux serveurs de mise à jour de Kaspersky Lab et à d'autres serveurs via un serveur proxy.</p>
	<p><b>Paramètres de mise à jour des modules de l'application</b></p>	<p>Vous pouvez indiquer les actions que Kaspersky Security for Windows Server va réaliser si des mises à jour critiques des modules de l'application sont disponibles ou ont déjà été installées et si Kaspersky Security for Windows Server doit obtenir des informations sur les mises à jour planifiées.</p>
	<p><b>Planification</b></p>	<p>Vous pouvez configurer les paramètres de lancement de la tâche planifiée.</p>



Configuration de l'analyse à la demande (cf. section "Création d'une tâche d'analyse à la demande" à la page <a href="#">488</a> ).	<b>Zone d'analyse</b>	Vous pouvez définir la zone d'analyse pour la tâche d'analyse à la demande et accéder à la configuration du niveau de sécurité.
	<b>Fenêtre Paramètres de l'analyse à la demande</b>	Dans la fenêtre <b>Paramètres de l'analyse à la demande</b> ouverte via le lien de la section <b>Zone d'analyse</b> , sélectionnez un des niveaux de sécurité prédéfinis ou personnalisez manuellement les paramètres du niveau de sécurité.
	<b>Options</b>	La zone de groupe <b>Analyse heuristique</b> vous permet d'activer ou de désactiver l'utilisation de l'analyseur heuristique pour la tâche d'analyse à la demande et de configurer le niveau d'analyse à l'aide d'un curseur. Vous pouvez configurer les paramètres suivants dans la zone de groupe <b>Intégration aux autres composants</b> : <ul style="list-style-type: none"> <li>• Appliquer la zone de confiance pour les tâches d'analyse à la demande.</li> <li>• Utilisation du KSN pour les tâches d'analyse à la demande.</li> <li>• Niveau de priorité de la tâche d'analyse à la demande : exécuter la tâche en arrière-plan (priorité basse) ou considérer l'exécution de la tâche comme un tâche d'analyse rapide.</li> </ul>
	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.
Vérification de l'intégrité de l'application (à la page <a href="#">135</a> )	<b>Planification</b>	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Pour la tâche Annulation de la mise à jour des bases de l'application, vous ne pouvez configurer que les paramètres de tâche standard dans les sections **Notification** et **Exclusions de la zone d'action de la tâche** gérées par Kaspersky Security Center.

Vous trouverez plus d'informations sur la configuration des paramètres dans ces sections dans le *Système d'aide de Kaspersky Security Center*.

## Dans cette section

Tâche Activation de l'application .....	<a href="#">133</a>
Tâches de mise à jour .....	<a href="#">133</a>
Vérification de l'intégrité de l'application .....	<a href="#">135</a>

## Tâche Activation de l'application

► Pour configurer la tâche Activation de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
  - Double-cliquez sur le nom de la tâche dans la liste des tâches créées ;
  - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche**.
  - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.
4. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le [Système d'aide de Kaspersky Security Center](#).

5. Dans la section **Paramètres d'activation**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter une clé pour renouveler la licence.
6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le [Système d'aide de Kaspersky Security Center](#).

9. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

## Tâches de mise à jour

► Pour configurer la tâche Copie des mises à jour, Mise à jour des bases de l'application ou Mise à jour des modules de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
  - Double-cliquez sur le nom de la tâche dans la liste des tâches créées ;
  - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche**.
  - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.
4. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

5. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
  - Dans la section **Source des mises à jour**, configurez les paramètres de la source des mises à jour et l'optimisation de l'utilisation du sous-système disque.
    - a. Dans la section **Source des mises à jour**, vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky Lab en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.  
  
Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky Lab en cas d'indisponibilité des serveurs personnalisés manuellement.
    - b. La section **Optimisation de l'utilisation des I/O du disque** permet de configurer les paramètres de la fonction réduisant la charge sur le sous-système disque pour la tâche Mise à jour des bases de l'application :
      - **Réduire la charge sur les I/O du disque**  
  
La case active ou désactive la fonction d'optimisation du sous-système disque grâce à un placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive.  
  
Si la case est cochée, la fonction est active.  
  
Cette case est décochée par défaut.
      - **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**  
  
Volume de mémoire vive (en mégaoctets) que l'application utilisera pour le placement des fichiers de mises à jour. Le volume de mémoire vive défini par défaut est de 512 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.
    - c. Cliquez sur le bouton **Paramètres de connexion** et, dans la fenêtre **Paramètres de connexion** qui s'ouvre, configurez les paramètres d'utilisation du serveur proxy pour la connexion avec les serveurs de mise à jour de Kaspersky Lab et d'autres serveurs.
  - La section **Paramètres de mise à jour des modules de l'application** pour la tâche Mise à jour des modules de l'application permet de désigner les actions que Kaspersky Security for Windows Server va effectuer si des mises à jour critiques des modules de l'application sont disponibles ou si des informations sur les mises à jour programmées sont disponibles. Elle permet également de configurer les actions effectuées par Kaspersky Security for Windows Server une fois l'installation des mises à jour

critiques terminée.

- Dans la section **Paramètres de copie des mises à jour** de la tâche Copie des mises à jour, désignez la composition des mises à jour et le dossier de destination.
6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
  7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

8. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

S'agissant de la tâche Annulation de la mise à jour des bases de l'application, vous pouvez configurer uniquement les paramètres de tâche standard contrôlée par Kaspersky Security Center dans les sections **Notifications** et **Exclusions de la zone d'analyse**. Vous trouverez plus d'informations sur la configuration des paramètres dans ces sections dans le *Système d'aide de Kaspersky Security Center*.

## Vérification de l'intégrité de l'application

► Pour configurer la tâche de groupe *Vérification de l'intégrité de l'application*, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
  - Double-cliquez sur le nom de la tâche dans la liste des tâches créées ;
  - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche**.
  - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.
4. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Périphériques**, choisissez les périphériques pour lesquels vous souhaitez configurer la tâche Vérification de l'intégrité de l'application.
6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

7. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le [Système d'aide de Kaspersky Security Center](#).

9. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.  
Les paramètres des tâches de groupe définis seront enregistrés.

## Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center

Si un problème survient durant l'utilisation de Kaspersky Security for Windows Server (par exemple, Kaspersky Security for Windows Server s'arrête suite à une erreur) et que vous souhaitez diagnostiquer le problème, vous pouvez activer la création de fichiers de trace et du fichier dump des processus de Kaspersky Security for Windows Server et envoyer ces fichiers au Support Technique de Kaspersky Lab pour l'analyse.

Kaspersky Security for Windows Server n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par l'utilisateur avec les droits correspondants.

Kaspersky Security for Windows Server consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Security for Windows Server. Vous pouvez configurer les autorisations d'accès (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)) et autoriser l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs requis.

► *Pour configurer les paramètres de diagnostic des échecs dans Kaspersky Security Center, procédez comme suit :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application** (cf. section "**Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center**" à la page [127](#)).
2. Ouvrez la section **Diagnostic des échecs**, puis procédez comme suit :
  - Si vous souhaitez enregistrer les informations de débogage dans un fichier, cochez la case **Consigner les informations de débogage dans le fichier de trace**.
    - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security for Windows Server va enregistrer les fichiers de trace.
    - Configurez le niveau de détail des informations de débogage.

Cette liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Security for Windows Server consigne dans le fichier de trace.

Vous avez le choix parmi les niveaux de détail suivants :

- **Événements critiques** : Kaspersky Security for Windows Server enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.
- **Erreurs** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
- **Événements importants** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.
- **Événements d'information** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs, aux événements importants et aux événements d'information.
- **Toutes les informations de débogage** : Kaspersky Security for Windows Server enregistre dans le fichier de trace toutes les informations de débogage.

Le niveau de détail à définir pour résoudre le problème qui se pose est déterminé par l'expert du Support Technique.

Le niveau de détail sélectionné par défaut est **Toutes les informations de débogage**.

La liste déroulante est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée.

- Taille maximale du fichier de trace
- Indiquez les modules à déboguer. Les codes des composants doivent être séparés par un point-virgule. Les codes sont sensibles à la case (cf. tableau ci-dessous).

Tableau 19. Codes de sous-système de Kaspersky Security for Windows Server

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Security for Windows Server dans Microsoft Management Console.
ak_conn	Sous-système d'intégration à l'Agent d'administration de Kaspersky Security Center
bl	Processus de contrôle, met en œuvre les tâches de contrôle de Kaspersky Security for Windows Server.
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance Kaspersky Security for Windows Server.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de Protection des fichiers en temps réel.
qb	Sous-système de la Quarantaine et de la Sauvegarde.
scandll	Module auxiliaire d'analyse antivirus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.

prague	Sous-système des fonctions de base.
updater	Sous-système de mise à jour des bases de données et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant logiciel enfichable de Kaspersky Security for Windows Server (gui) et du plug-in d'administration de Kaspersky Security Center (ak\_conn) sont appliqués après le redémarrage de ces composants. Les paramètres de traçage des sous-systèmes de prise en charge du protocole SNMP (snmp) sont appliqués après le relancement du service SNMP. Les paramètres de traçage du sous-système des compteurs de performance (perfcount) sont appliqués après le relancement de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Security for Windows Server sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Par défaut, Kaspersky Security for Windows Server consigne les informations de débogage pour tous les composants de Kaspersky Security for Windows Server.

Le champ est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée

- Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump**.
  - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security for Windows Server enregistrera le fichier dump.

3. Cliquez sur le bouton **OK**.

Les paramètres configurés de l'application seront appliqués sur le serveur protégé.

## Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Security for Windows Server et configurer les paramètres de la planification.

### Dans cette section

Configuration des paramètres de la planification du lancement de la tâche .....	<a href="#">138</a>
Activation et désactivation du lancement programmé .....	<a href="#">140</a>

## Configuration des paramètres de la planification du lancement de la tâche

La console de l'application permet de planifier le lancement des tâches locales du système et définies par l'utilisateur. Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement de la tâche de groupe, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.



2. Sélectionnez le groupe auquel appartient le serveur protégé.
3. Dans le panneau de détails, choisissez l'onglet **Tâches**.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
  - Double-cliquez sur le nom de la tâche.
  - Ouvrez le menu contextuel du nom de la tâche et sélectionnez l'option Propriétés.
5. Sélectionnez la section **Planification**.
6. Dans le groupe **Paramètres de planification**, cochez la case **Exécuté selon la programmation**.

Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée est interdite par une stratégie de Kaspersky Security Center.

7. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
  - a. Choisissez une des options suivantes dans la liste **Fréquence** :
    - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
    - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
    - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;
    - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security for Windows Server.
    - **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.
  - b. Indiquez, dans le champ **Démarrer à**, l'heure du premier lancement de la tâche.
  - c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

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, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est interdit par les paramètres d'une stratégie active de Kaspersky Security Center (cf. section "Configuration de la planification de l'exécution programmée des tâches locales du système" à la page. [104](#)).

8. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.
  - Dans la section **Paramètres d'arrêt de la tâche** :
    - a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la tâche.

- b. Cochez la case **Pause à partir de**, puis saisissez les heures de début et de fin pour spécifier un intervalle de temps de moins de 24 heures pendant lequel l'exécution de la tâche sera suspendue.
- Dans la section **Paramètres avancés** :
  - a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.
  - b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.
  - c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.
9. Cliquez sur le bouton **OK**.
10. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

Si vous souhaitez configurer les paramètres de l'application pour une tâche unique à l'aide de Kaspersky Security Center, suivez les étapes décrites à la section Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center (à la page [127](#)).

## Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver le lancement des tâches planifiées après ou avant la configuration de la planification.

► *Pour activer ou désactiver la planification du lancement de la tâche, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nom de la tâche dont vous souhaitez planifier le lancement.
2. Choisissez l'option **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

3. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes sous l'onglet **Planification** :
  - Cochez la case **Exécuté selon la programmation** si vous souhaitez activer l'exécution planifiée d'une tâche.
  - Décochez la case **Exécuté selon la programmation** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

Les paramètres de la planification du lancement de la tâche ne sont pas supprimés. Ils sont appliqué au prochain lancement planifié de la tâche.

4. Cliquez sur le bouton **OK**.
5. Cliquez sur le bouton **Appliquer**.

Les paramètres configurés de la planification du lancement de la tâche sont enregistrés.

## Génération de rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils

sont basés sur les informations stockées sur le serveur d'administration.

A partir de la version Kaspersky Security Center 11, les types de rapport suivants sont disponibles pour Kaspersky Security for Windows Server :

- Rapport sur l'état des composants de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Consultez l'[aide de Kaspersky Security Center](#) pour obtenir des informations détaillées sur tous les rapports de Kaspersky Security Center et la manière de les configurer.

### Rapport sur l'état des composants de l'application

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée du composant défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque composant : *Exécution en cours*, *En pause*, *Arrêté*, *Dysfonctionnement*, *Pas installé*, *Démarrage en cours*.

L'état *Non installé* désigne le composant, et non l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de composants et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de composants et leur état

Cf. [Aide de Kaspersky Security Center](#) pour plus de détails sur la création et l'utilisation de sélections.

#### ► Pour consulter les états des composants dans les paramètres de l'application :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).
3. Sélectionnez la section **Composants**.
4. Consultez le tableau d'état.

#### ► Pour consulter un rapport standard Kaspersky Security Center :

1. Sélectionnez le nœud **Serveur d'administration <nom de l'ordinateur>** dans l'arborescence de la Console d'administration.
2. Ouvrez l'onglet **Rapports**.

3. Double-cliquez sur l'élément de liste **Rapport sur l'état des composants de l'application**.  
Un rapport est généré.
4. Examinez les détails suivants du rapport :
  - Diagramme graphique.
  - Tableau récapitulatif des composants et nombres totaux d'appareils de réseau où chacun des composants est installé et groupes auxquels ils appartiennent.
  - Tableau détaillé spécifiant l'état des composants, la version, l' et le groupe.

### Rapports sur les applications bloquées dans les modes actifs et statistiques

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications, deux types de rapports peuvent être générés : rapport sur les applications interdites (si la tâche est démarrée en mode Actif), rapport sur les applications interdites en mode test (si la tâche est démarrée en mode Statistiques uniquement). Ces rapports affichent des informations sur les applications interdites sur les serveurs protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky Lab installées sur les appareils protégés.

#### ► Pour consulter un rapport sur les applications interdites en mode test :

1. Démarrez la tâche Contrôle des applications en mode Statistiques uniquement (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page [373](#)).
2. Sélectionnez le nœud **Serveur d'administration <nom de l'ordinateur>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur l'élément de liste **Rapport sur les applications interdites en mode test**.  
Un rapport est généré.
5. Examinez les détails suivants du rapport :
  - Diagramme graphique qui affiche les dix application avec la plus grande quantité de démarrages bloqués.
  - Tableau récapitulatif des interdictions d'applications survenues spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
  - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

#### ► Pour afficher un rapport sur les applications interdites en mode Actif :

1. Démarrez la tâche Contrôle des applications en mode Actif (cf. section "Configuration des paramètres de la tâche Contrôle du lancement des applications" à la page [373](#)).
2. Sélectionnez le nœud **Serveur d'administration <nom de l'ordinateur>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur un élément de liste **Rapport sur les applications interdites**.  
Un rapport est généré.

Ce rapport comprend les mêmes blocs de données que le rapport sur les applications interdites en mode test.

# Utilisation de la console de Kaspersky Security for Windows Server

Cette section fournit des informations sur la console de Kaspersky Security for Windows Server et sur l'administration de l'application via la console de l'application installée sur le serveur protégé ou sur un autre ordinateur.

## Contenu du chapitre

Paramètres de Kaspersky Security for Windows Server dans la Console de l'application .....	<a href="#">143</a>
A propos de la console de Kaspersky Security for Windows Server .....	<a href="#">150</a>
Interface de la console de Kaspersky Security for Windows Server .....	<a href="#">151</a>
Icône de la barre d'état système dans la zone de notification .....	<a href="#">154</a>
Administration de Kaspersky Security for Windows Server via la Console de l'application sur un autre ordinateur .....	<a href="#">156</a>
Administration des tâches de Kaspersky Security for Windows Server .....	<a href="#">156</a>
Consultation de l'état de la protection et des informations de Kaspersky Security for Windows Server .....	<a href="#">167</a>
Interface de diagnostic compacte .....	<a href="#">173</a>
Mise à jour des bases de données et des modules de l'application Kaspersky Security for Windows Server ....	<a href="#">178</a>
Isolement et copie de sauvegarde des objets .....	<a href="#">193</a>
Enregistrement des événements.Journaux de Kaspersky Security for Windows Server .....	<a href="#">213</a>
Configuration des notifications.....	<a href="#">227</a>

## Paramètres de Kaspersky Security for Windows Server dans la Console de l'application

Les paramètres généraux et les paramètres du diagnostic des pannes de Kaspersky Security for Windows Server définissent les conditions générales de fonctionnement de l'application. Ils déterminent le nombre de processus que Kaspersky Security for Windows Server va utiliser, ils permettent d'activer la reprise des tâches de Kaspersky Security for Windows Server après un arrêt inopiné de leur fonctionnement, de tenir un journal de traçage, d'activer la création d'un fichier dump des processus de Kaspersky Security for Windows Server lorsqu'ils sont arrêtés en raison d'une erreur et de configurer d'autres paramètres généraux.

La configuration des paramètres du fonctionnement de l'application dans la console de l'application n'est pas disponible si la modification de ces paramètres est interdite dans la stratégie active de Kaspersky Security Center.

► *Pour configurer les paramètres de Kaspersky Security for Windows Server :*

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Security** et réalisez

l'une des actions suivantes :

- Dans le panneau de détails du nœud, suivez le lien **Propriétés de l'application**.
- Dans le menu contextuel du nœud, sélectionnez l'option **Propriétés**.

La fenêtre **Paramètres de l'application** s'ouvre.

2. Dans la fenêtre qui s'ouvre, configurez les paramètres généraux de Kaspersky Security for Windows Server en fonction de vos préférences :

- L'onglet **Montée en puissance et interface** permet de configurer les paramètres suivants :
  - Dans la section **Paramètres d'optimisation** :
    - nombre maximum de processus de travail que Kaspersky Security for Windows Server peut lancer ;

Tableau 20. Quantité maximale de processus actifs

Paramètre	Quantité maximale de processus actifs	
<b>Description</b>	<p>Ce paramètre appartient au groupe <b>Paramètres d'optimisation</b> de Kaspersky Security for Windows Server. Il définit le nombre maximum de processus actifs qui peuvent être exécutés simultanément par l'application.</p> <p>L'augmentation du nombre de processus exécutés en parallèle accélère la vitesse d'analyse des fichiers et la résistance de Kaspersky Security for Windows Server aux échecs. Toutefois, si cette valeur est trop élevée, les performances globales du serveur peuvent chuter et la mémoire vive requise peut augmenter.</p> <p>N'oubliez pas que la Console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre <b>Quantité maximale de processus actifs</b> uniquement pour Kaspersky Security for Windows Server sur un ordinateur séparé (dans la boîte de dialogue <b>Paramètres de l'application</b>) ; vous ne pouvez toutefois pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe d'ordinateurs.</p>	
<b>Valeurs possibles</b>	1 – 8	
<b>Valeur par défaut</b>	L'application réalise une montée en capacité automatique en fonction du nombre de processeurs sur l'ordinateur :	
	<b>Nombre de processeurs</b>	<b>Quantité maximale de processus actifs</b>
	1	1
	1 < nombre de processeurs < 4	2
	4 et plus	4

- Nombre de processus pour la protection de l'ordinateur en temps réel

Tableau 21. Nombre de processus de protection en temps réel

Paramètre	Nombre de processus de protection en temps réel						
<b>Description</b>	<p>Ce paramètre appartient au groupe <b>Paramètres d'optimisation</b> de Kaspersky Security for Windows Server.</p> <p>Grâce à ce paramètre, vous pouvez définir le nombre fixe de processus qui serviront à Kaspersky Security for Windows Server pour l'exécution des tâches de protection en temps réel.</p> <p>La valeur plus élevée de ce paramètre accélère l'analyse des objets dans les tâches de protection en temps réel. Toutefois, plus le nombre de processus affectés à Kaspersky Security for Windows Server est élevé, plus l'impact sur les performances globales de l'ordinateur protégé et sur son utilisation de la mémoire vive sera marqué.</p> <p>N'oubliez pas que la Console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre <b>Nombre de processus de protection en temps réel</b> uniquement pour Kaspersky Security for Windows Server sur un ordinateur distinct (dans la boîte de dialogue <b>Paramètres de l'application</b>) ; vous ne pouvez pas toutefois pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe d'ordinateurs.</p>						
<b>Valeurs possibles</b>	<p>Valeurs possibles : 1-N, où N est la valeur définie par le paramètre <b>Quantité maximale de processus actifs</b>.</p> <p>Si vous attribuez au paramètre <b>Nombre de processus de protection en temps réel</b> une valeur égale au nombre maximum de processus actifs, vous diminuez l'impact de Kaspersky Security for Windows Server sur la vitesse de l'échange de fichiers entre les postes de travail et l'ordinateur, ce qui améliore les performances de 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 <b>Moyenne</b> (Normal) sont exécutées dans les processus de Kaspersky Security for Windows Server déjà lancés. Les tâches d'analyse à la demande seront exécutées plus lentement. Si l'exécution de la tâche entraîne un échec, son relancement prendra plus de temps.</p> <p>Les tâches d'analyse à la demande avec la priorité de base <b>faible</b> (Low) sont toujours exécutées dans un ou plusieurs processus séparés.</p>						
<b>Valeur par défaut</b>	<p>Kaspersky Security for Windows Server réalise une montée en capacité automatique en fonction du nombre de processeurs sur l'ordinateur :</p> <table border="1"> <thead> <tr> <th>Nombre de processeurs</th> <th>Nombre de processus de protection en temps réel</th> </tr> </thead> <tbody> <tr> <td>=1</td> <td>1</td> </tr> <tr> <td>&gt;1</td> <td>2</td> </tr> </tbody> </table>	Nombre de processeurs	Nombre de processus de protection en temps réel	=1	1	>1	2
Nombre de processeurs	Nombre de processus de protection en temps réel						
=1	1						
>1	2						



- Nombre de processus de travail pour les tâches d'analyse à la demande en arrière-plan

Tableau 22. Nombre de processus pour les tâches d'analyse à la demande en arrière-plan

Paramètre	Nombre de processus pour les tâches d'analyse à la demande en arrière-plan
<b>Description</b>	<p>Ce paramètre appartient au groupe <b>Paramètres d'optimisation</b> de Kaspersky Security for Windows Server.</p> <p>Grâce à ce paramètre, vous pouvez définir le nombre maximum de processus que l'application va utiliser pour l'exécution des tâches d'analyse à la demande en arrière-plan.</p> <p>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 Security for Windows Server défini à l'aide du paramètre <b>Quantité maximale de processus actifs</b>.</p> <p>Par exemple, si vous spécifiez les valeurs des paramètres comme ci-dessous :</p> <ul style="list-style-type: none"> <li>• Quantité maximale de processus actifs – 3 ;</li> <li>• Nombre de processus pour les tâches de protection en temps réel – 3 ;</li> <li>• Nombre de processeurs pour les tâches d'analyse à la demande en arrière-plan – 1 ;</li> </ul> <p>et puis que vous lancez des tâches de protection en temps réel et une tâche d'analyse à la demande en arrière-plan, le nombre total de processus kavfswp.exe de Kaspersky Security for Windows Server est de 4.</p> <p>Un processus de travail de faible priorité peut exécuter plusieurs tâches d'analyse à la demande.</p> <p>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 ainsi que la vitesse.</p>
<b>Valeurs possibles</b>	1-4
<b>Valeur par défaut</b>	1

- Dans la section **Interaction avec l'utilisateur**, décidez d'afficher ou non l'icône de la barre d'état système dans la barre de tâches après chaque lancement de l'application (cf. section "Icône de la barre d'état dans la zone de notification" à la page [154](#)).
- L'onglet **Sécurité et fiabilité** permet de configurer les paramètres suivants :
  - Dans la section **Paramètres de fiabilité**, indiquez le nombre de tentatives de restauration des tâches d'analyse à la demande en cas d'échec suite à une erreur.

Tableau 23. Récupération automatique

<b>Paramètre</b>	Restauration des tâches ( <b>Réaliser la restauration des tâches</b> ).
<b>Description</b>	<p>Ce paramètre appartient au groupe <b>Paramètres de fiabilité</b> de Kaspersky Security for Windows Server. 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.</p> <p>Lorsqu'une tâche se solde par un échec, le processus kavfs.exe de Kaspersky Security for Windows Server tente de relancer le processus dans lequel cette tâche était exécutée au moment de l'arrêt.</p> <p>Si la restauration des tâches est désactivée, l'application ne restaure pas les tâches Protection en temps réel et Analyse à la demande.</p> <p>Si la restauration des tâches est activée, l'application 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.</p>
<b>Valeurs possibles</b>	<p>Activée / désactivée.</p> <p>Nombre de tentatives de restauration des tâches d'analyse à la demande : 1 - 10.</p>
<b>Valeur par défaut</b>	La restauration des tâches est activée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 2

- La section **Action lors du passage à une source d'alimentation continue** permet de choisir les actions de Kaspersky Security for Windows Server dans le cadre de l'alimentation de secours.

Tableau 24. Utilisation de la source d'alimentation de secours

<b>Paramètre</b>	Actions à exécuter en cas d'alimentation via l'alimentation de secours
<b>Description</b>	Ce paramètre définit les actions exécutées par Kaspersky Security for Windows Server lorsque l'ordinateur fonctionne sur l'alimentation électrique de secours.
<b>Valeurs possibles</b>	<p>Lancer ou pas les tâches d'analyse à la demande qui ont été programmées ;</p> <p>Exécuter ou arrêter toutes les tâches d'analyse à la demande actives.</p>
<b>Valeur par défaut</b>	<p>Par défaut, lorsque l'ordinateur utilise une source d'alimentation de secours, Kaspersky Security for Windows Server fonctionne selon le mode suivant :</p> <ul style="list-style-type: none"> <li>• N'exécute pas les tâches d'analyse à la demande qui ont été programmées.</li> <li>• Arrête automatiquement toutes les tâches d'analyse à la demande actives.</li> </ul>

- Dans la section **Paramètres de protection par mot de passe**, configurez les paramètres pour la protection par mot de masse des fonctions de l'application (cf. section "Accès protégé par mot de passe aux fonctions de Kaspersky Security for Windows Server" à la page [246](#)).
- Sous l'onglet **Paramètres de connexion** :
  - Définissez les paramètres d'utilisation du serveur proxy dans la section **Paramètres du serveur proxy**.
  - Dans la section **Paramètres d'authentification du serveur proxy**, indiquez le type

d'authentification et les données requises pour l'authentification sur le serveur proxy.

- Dans la section **Licence**, indiquez si Kaspersky Security Center doit être utilisé en guise de serveur proxy pour l'activation de l'application.
- Sous l'onglet **Diagnostic des échecs** :
  - Si vous souhaitez enregistrer les informations de débogage dans un fichier, cochez la case **Consigner les informations de débogage dans le fichier de trace**.
    - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security for Windows Server va enregistrer les fichiers de trace.
    - Configurez le niveau de détail des informations de débogage.

Cette liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Security for Windows Server consigne dans le fichier de trace.

Vous avez le choix parmi les niveaux de détail suivants :

- **Événements critiques** : Kaspersky Security for Windows Server enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.
- **Erreurs** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
- **Événements importants** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.
- **Événements d'information** : Kaspersky Security for Windows Server enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs, aux événements importants et aux événements d'information.
- **Toutes les informations de débogage** : Kaspersky Security for Windows Server enregistre dans le fichier de trace toutes les informations de débogage.

Le niveau de détail à définir pour résoudre le problème qui se pose est déterminé par l'expert du Support Technique.

Le niveau de détail sélectionné par défaut est **Toutes les informations de débogage**.

La liste déroulante est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée.

- Taille maximale du fichier de trace
- Indiquez les modules à déboguer.

Liste des codes des composants de Kaspersky Security for Windows Server dont les informations de débogage sont enregistrées dans le fichier de trace. Les codes des composants doivent être séparés par un point-virgule. Les codes sont sensibles à la case (cf. tableau ci-dessous).

Tableau 25. Codes de sous-système de Kaspersky Security for Windows Server

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Security for Windows Server dans Microsoft Management Console.
ak_conn	Sous-système d'intégration à l'Agent d'administration de Kaspersky Security Center

bl	Processus de contrôle, met en œuvre les tâches de contrôle de Kaspersky Security for Windows Server.
wp	Processus de travail ; exécute la tâche de protection antivirus
blgate	Processus d'administration à distance Kaspersky Security for Windows Server.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de Protection des fichiers en temps réel.
qb	Sous-système de la Quarantaine et de la Sauvegarde.
scandll	Module auxiliaire d'analyse antivirus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.
prague	Sous-système des fonctions de base.
updater	Sous-système de mise à jour des bases de données et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant logiciel enfichable de Kaspersky Security for Windows Server (gui) et du plug-in d'administration de Kaspersky Security for Windows Server pour Kaspersky Security Center (ak\_conn) sont appliqués après le redémarrage de ces composants. Les paramètres de traçage des sous-systèmes de prise en charge du protocole SNMP (snmp) sont appliqués après le relancement du service SNMP. Les paramètres de traçage du sous-système des compteurs de performance (perfcount) sont appliqués après le relancement de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Security for Windows Server sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Par défaut, Kaspersky Security for Windows Server consigne les informations de débogage pour tous les composants de Kaspersky Security for Windows Server.

Le champ est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée

- Si vous souhaitez que l'application crée un fichier dump, cochez la case **Créer un fichier dump lors d'un incident**.

Kaspersky Security for Windows Server n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par l'utilisateur avec les droits correspondants.

- Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Security for Windows Server enregistrera le fichier dump.

Kaspersky Security for Windows Server consigne les informations dans les fichiers de trace et les fichiers dump en clair. Le dossier d'enregistrement des fichiers est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Security for Windows Server. Vous pouvez configurer les autorisations d'accès (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)) et autoriser l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs requis.

3. Cliquez sur le bouton **OK**.

Les paramètres de Kaspersky Security for Windows Server sont enregistrés.

## A propos de la console de Kaspersky Security for Windows Server

La console de Kaspersky Security for Windows Server est un composant logiciel enfichable isolé qui est ajouté à la console Microsoft Management Console.

Il est possible d'administrer l'application via la console de l'application installée sur le serveur protégé ou sur un autre ordinateur du réseau de l'organisation.

Après que la Console de l'application a été installée sur un autre ordinateur, il faut réaliser une configuration avancée.

Si la console de l'application et Kaspersky Security for Windows Server sont installés sur différents ordinateurs appartenant à différents domaines, il se peut qu'il y ait des restrictions au niveau de la remise des informations de l'application à la console de l'application. Par exemple, après le démarrage d'une tâche quelconque de l'application, il se peut que l'état de cette tâche reste inchangé dans la console de l'application.

Lors de l'installation de la console de l'application, l'assistant d'installation crée le fichier kavfs.msc dans le répertoire d'installation et ajoute le composant logiciel enfichable Kaspersky Security for Windows Server à la liste des composants logiciels enfichables isolés de Microsoft Windows.

Vous pouvez démarrer la console de l'application depuis le menu **Démarrer**. Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Security for Windows Server ou l'ajouter à la console Microsoft Management Console existante en tant que nouvel élément de son arborescence.

Sous la version 64 bits de Microsoft Windows, vous pouvez ajouter le composant logiciel enfichable de Kaspersky Security for Windows Server uniquement dans la console Microsoft Management Console de la version 32 bits. Pour ce faire, tapez la commande `mmc.exe/32` dans la ligne de commande pour ouvrir la Microsoft Management Console.

Dans une des consoles Microsoft Management Console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants logiciels enfichables Kaspersky Security for Windows Server afin de pouvoir administrer ainsi la protection de plusieurs serveurs sur lesquels Kaspersky Security for Windows Server est installé.

## Interface de la console de Kaspersky Security for Windows Server

La Console de Kaspersky Security for Windows Server s'affiche dans l'arborescence de Microsoft Management Console en tant que nœud nommé Kaspersky Security.

Après la connexion à la copie de Kaspersky Security for Windows Server installée sur un autre serveur, le nom du nœud reprend le nom du serveur sur lequel l'application est installée et le nom du compte utilisateur sous les privilèges duquel la connexion a été réalisée : **Kaspersky Security <nom du serveur> comme <nom de compte>**. En cas de connexion à une instance de Kaspersky Security for Windows Server installée sur le même serveur que la console de l'application, le nom du nœud devient **Kaspersky Security**.

Par défaut, la fenêtre de la console de l'application contient les éléments suivants :

- Arborescence de la console de l'application
- Panneau des résultats
- Barre d'outils.

### Arborescence de la console de l'application

L'arborescence de la console de l'application affiche le nœud **Kaspersky Security** et ses nœud enfant correspondant aux composants opérationnels de l'application.

Le nœud **Kaspersky Security** inclut les nœuds enfant suivants :

- **Protection en temps réel du serveur** : administration des tâches de protection en temps réel et des services KSN. Le nœud **Protection en temps réel du serveur** permet de configurer les tâches suivantes :
  - **Protection des fichiers en temps réel**
  - **Monitoring des scripts**
  - **Utilisation du KSN**
  - **Protection du trafic**
  - **Protection contre le chiffrement**
- **Contrôle du serveur** : contrôle les lancements des applications installées ainsi que les connexions des périphériques externes. Le nœud **Contrôle du serveur** permet de configurer les tâches suivantes :
  - **Contrôle du lancement des applications**
  - **Contrôle des périphériques**
  - **Gestion du pare-feu**
- **Génération automatique de règles** : configuration de la création automatique des règles de groupe et système pour les tâches Contrôle du lancement des applications et Contrôle des périphériques.
  - **Génération des règles du Contrôle du lancement des applications**
  - **Génération des règles du Contrôle des périphériques ;**
  - Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).

Les tâches de groupe (cf. section "Catégories des tâches de Kaspersky Security for Windows Server" à la page [156](#)) sont créées à l'aide de Kaspersky Security Center. Il est impossible d'administrer des tâches de groupe via la console de l'application.

- **Diagnostic du système** : configuration des paramètres du contrôle des opérations réalisées sur les fichiers

et de l'inspection des journaux des événements Windows.

- **Moniteur d'intégrité des fichiers**
- **Inspection des journaux**
- **Protection des stockages réseau** : configurez les tâches de protection des stockage réseau.
  - **Protection RPC des stockages réseau connectés**
  - **Protection ICAP des stockages réseau connectés**
  - **Protection contre le chiffrement pour NetApp**
- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Un nœud séparé existe pour chacune des tâches :
  - **Analyse au démarrage du système d'exploitation**
  - **Analyse des zones critiques**
  - **Analyse de la quarantaine**
  - **Vérification de l'intégrité de l'application**
  - Tâches définies par l'utilisateur **<Nom des tâches>** (le cas échéant).

Le nœud affiche les tâches système (cf. section "Catégories des tâches de Kaspersky Security for Windows Server" à la page [156](#)) créées lors de l'installation de l'application, les tâches définies par l'utilisateur ainsi que les tâches de groupe d'analyse à la demande créées et transmises à l'ordinateur à l'aide de Kaspersky Security Center.

- **Mise à jour** : gère la mise à jour des bases de données et des modules de Kaspersky Security for Windows Server ainsi que la copie des mises à jour dans le dossier de la source locale de mises à jour. Le nœud contient des nœuds enfants permettant d'administrer chacune des tâches de mise à jour et la dernière annulation de la mise à jour des bases de l'application :
  - **Mise à jour des bases de l'application**
  - **Mise à jour des modules de l'application**
  - **Copie des mises à jour**
  - **Annulation de la mise à jour des bases de l'application**

Le nœud affiche toutes les tâches définies par l'utilisateur et les tâches de groupe (cf. section "Catégories des tâches de Kaspersky Security for Windows Server" à la page [156](#)) de mise à jour créées et transmises à l'ordinateur via Kaspersky Security Center.

- **Stockages** : administration des paramètres de la quarantaine, de la Sauvegarde et des ordinateurs bloqués.
  - **Quarantaine**
  - **Sauvegarde**
  - **Liste des ordinateurs bloqués**
- **Journaux et notifications** : gestion des journaux d'exécution des tâches locales, du journal de sécurité et du journal d'audit système de Kaspersky Security for Windows Server.
  - **Journaux de sécurité**
  - **Journal d'audit système**



- **Journaux d'exécution de la tâche**
- **Licence** : ajout et suppression de clés et de codes d'activation pour Kaspersky Security for Windows Server, consultation des informations relatives aux licences.

### Panneau des résultats

Le panneau de détails reprend les informations relatives au nœud sélectionné. Si vous avez choisi le nœud **Kaspersky Security**, le panneau de détails affiche les informations relatives à l'état actuel de la protection du serveur (cf. section "Consultation de l'état de la protection et des informations sur Kaspersky Security for Windows Server" à la page [167](#)), les informations relatives à Kaspersky Security for Windows Server, l'état de la protection de ses composants fonctionnels et la date d'expiration de la licence.

### Menu contextuel du nœud Kaspersky Security

A l'aide des options du menu contextuel du nœud **Kaspersky Security**, vous pouvez exécuter les opérations suivantes :

- **Se connecter à un autre ordinateur.** Se connecter à un autre ordinateur (cf. section "Administration de Kaspersky Security for Windows Server via la console de l'application sur un autre ordinateur" à la page [156](#)) pour administrer la version de Kaspersky Security for Windows Server qui y est installée. Pour effectuer cette opération, vous pouvez également cliquer sur le lien situé dans le coin inférieur droit du panneau de détails du nœud **Kaspersky Security**.
- **Démarrer le service / Arrêter le service.** Lancer ou arrêter l'application ou la tâche sélectionnée (cf. section "Lancement / suspension / rétablissement / arrêt manuel des tâches" à la page [157](#)). Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. L'exécution de ces opérations est également disponible dans les menus contextuels des tâches de l'application.
- **Configurer l'analyse des disques amovibles.** Configurez l'analyse des disques amovibles (cf. section "A propos de l'analyse des disques amovibles" à la page [483](#)) connectés au serveur protégé via le port USB.
- **Protection contre les exploits : paramètres généraux.** Configurez le mode Protection contre les exploits et configurez des actions de prévention.
- **Protection contre les exploits : paramètres de protection des processus.** Ajoutez les processus à protéger et sélectionnez les techniques de protection contre les exploits (cf. section "Technique de protection contre les exploits" à la page [544](#)).
- **Configurer les paramètres de la zone de confiance.** Consultez et configurez les paramètres de la zone de confiance (cf. section "A propos de la zone de confiance" à la page [520](#)).
- **Modifier les permissions utilisateur pour l'administration de l'application.** Consultez et configurez les autorisations d'accès aux fonctions de Kaspersky Security for Windows Server (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)).
- **Modifier les droits d'utilisateurs pour l'administration de Service Kaspersky Security.** Consultez et configurez les autorisations des utilisateurs pour l'administration du Service Kaspersky Security (cf. section "Configuration des autorisations d'accès à l'administration de Kaspersky Security for Windows Server et au service Kaspersky Security for Windows Server" à la page [244](#)).
- **Stockage hiérarchique.** Configurez la méthode d'accès du système HSM (cf. section "Configuration de paramètres du système HSM via la Console de l'application" à la page [547](#)).
- **Exporter les paramètres.** Enregistrez les paramètres de l'application dans un fichier de configuration au format XML (cf. section "Exportation des paramètres" à la page [163](#)). L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Importer les paramètres.** Importez les paramètres de l'application depuis le fichier de configuration au format XML (cf. section "Importation des paramètres" à la page [163](#)). L'exécution de cette opération est

également disponible dans les menus contextuels des tâches de l'application.

- **Données sur les mises à jour disponibles pour l'application et ses modules.** Affiche les informations relatives à Kaspersky Security for Windows Servers et aux mises à jour des modules de l'application disponibles.
- **Actualiser.** Actualisez le contenu de la fenêtre de la console de l'application. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Propriétés.** Consultez et configurez les paramètres de fonctionnement de Kaspersky Security for Windows Server ou d'une tâche sélectionnée. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Pour exécuter cette opération, vous pouvez également utiliser le lien **Propriétés de l'application** dans le panneau de détails du nœud **Kaspersky Security** ou le bouton dans la barre d'outils.

- **Aide.** Consultez les informations reprises dans l'aide de Kaspersky Security for Windows Server. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.


### Barre d'outils et menu contextuel des tâches de Kaspersky Security for Windows Server

Vous pouvez administrer les tâches de Kaspersky Security for Windows Server à l'aide des options du menu contextuel de chaque tâche dans l'arborescence de la console de l'application.

A l'aide des options du menu contextuel de la tâche sélectionnée, vous pouvez exécuter les opérations suivantes :



- **Reprendre / Suspendre.** Reprend ou suspend l'exécution d'une tâche (cf. section "Lancement / suspension / rétablissement / arrêt manuel des tâches" à la page [157](#)). Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches de protection en temps réel et d'analyse à la demande.
- **Ajouter une tâche.** Crée une tâche définie par l'utilisateur (cf. section "Création et configuration d'une tâche d'analyse à la demande" à la page [503](#)). L'opération est disponible pour les tâches d'analyse à la demande.
- **Ouvrir le journal.** Consultez et administrez un journal d'exécution de la tâche (cf. section "A propos du journal d'exécution de la tâche" à la page [216](#)). Cette opération est disponible pour toutes les tâches.
- **Enregistrer la tâche.** Enregistrez et appliquez les modifications apportées aux paramètres de la tâche. Cette action est disponible pour les tâches Protection des fichiers en temps réel et Analyse à la demande.
- **Supprimer la tâche.** Supprimez une tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.
- **Statistiques.** Accéder à la consultation des statistiques de la tâche. L'opération est disponible pour la tâche de vérification de l'intégrité de l'application.
- **Modèles des paramètres.** Administrez les modèles (cf. section "Utilisation des modèles de paramètres de sécurité" à la page [164](#)). Cette opération est disponible pour les tâches Protection des fichiers en temps réel et Analyse à la demande.

## Icône de la barre d'état système dans la zone de notification

Chaque fois que Kaspersky Security for Windows Server se lance automatiquement après le redémarrage de l'ordinateur, l'icône de la barre d'état système apparaît dans la zone de notification de la barre d'outils . L'icône est affichée par défaut si vous avez installé le composant Icône dans la barre d'état système lors de l'installation de

l'application.

L'apparence de l'icône de la barre d'état système indique l'état actuel de la protection du serveur. Les deux états sont possibles :

-  actif (icône colorée) si au moins une des tâches est en cours d'exécution : Protection des fichiers en temps réel, Contrôle du lancement des applications
-  inactif (icône en noir et blanc) si aucune des tâches est en cours d'exécution : Protection des fichiers en temps réel, Contrôle du lancement des applications

Vous pouvez ouvrir le menu contextuel de l'icône de la barre d'état système d'un clic droit de la souris.

Le menu contextuel contient plusieurs commandes d'affichage de fenêtre de l'application (cf. tableau ci-après).

Tableau 26. Commandes du menu contextuel affichées dans l'icône de la barre d'état système

Instruction	Description
<b>Ouvrir la Console de l'application</b>	Ouvrez la console de Kaspersky Security for Windows Server (si celle-ci est installée).
<b>Ouvrir l'interface de diagnostic compacte</b>	Ouvrez l'interface de diagnostic compacte.
<b>A propos de l'application</b>	Ouvre la fenêtre A propos de l'application qui contient des informations sur Kaspersky Security for Windows Server. Si vous êtes un utilisateur enregistré de Kaspersky Security for Windows Server, la fenêtre A propos de l'application contient des informations sur les mises à jour urgentes installées.
<b>Fermer</b>	Masque l'icône de la barre d'état système dans la zone de notification de la barre des tâches.

Vous pouvez à tout moment restaurer l'icône masquée de la barre d'état système.

► *Pour afficher à nouveau l'icône de l'application,*

dans le menu **Démarrer** de Microsoft Windows, sélectionnez **Tous les programmes > Kaspersky Security for Windows Server > Icône dans la barre d'état système**.

Les noms des paramètres peuvent varier selon les versions du système d'exploitation installé.

Lors de la configuration des paramètres généraux de Kaspersky Security for Windows Server, vous pouvez activer ou désactiver l'affichage de l'icône de la barre d'état système lors de chaque lancement automatique de l'application après un redémarrage du serveur.

## Administration de Kaspersky Security for Windows Server via la Console de l'application sur un autre ordinateur

Il est possible d'administrer Kaspersky Security for Windows Server via la console de l'application installée sur un ordinateur distant.

Pour administrer l'application via la console de Kaspersky Security for Windows Server sur un ordinateur distant, confirmez que :

- Les utilisateurs de la console de l'application sur l'ordinateur distant sont ajoutés au groupe KAVWSEE Administrators sur le serveur protégé.
- Les connexions réseau sont autorisées pour le processus du service Kaspersky Security Management (kavfsgt.exe), si le Pare-feu Windows est activé sur le serveur protégé.
- La case **Autoriser l'accès à distance** a été cochée dans la fenêtre de l'Assistant d'installation lors de l'installation de Kaspersky Security for Windows Server.

Si Kaspersky Security for Windows Server sur l'ordinateur distant est protégé par un mot de passe, vous devez le saisir pour accéder à l'administration de l'application via la console de l'application.

## Administration des tâches de Kaspersky Security for Windows Server

Cette section contient des informations sur les tâches de Kaspersky Security for Windows Server, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

### Dans cette section

Catégories de tâche de Kaspersky Security for Windows Server .....	<a href="#">156</a>
Lancement / suspension / rétablissement / arrêt manuel des tâches .....	<a href="#">157</a>
Programmation des tâches .....	<a href="#">157</a>
Utilisation des comptes utilisateur pour l'exécution des tâches .....	<a href="#">159</a>
Importation et exportation des paramètres .....	<a href="#">161</a>
Utilisation des modèles de paramètres de sécurité .....	<a href="#">164</a>

## Catégories de tâche de Kaspersky Security for Windows Server

Les fonctions de la protection en temps réel du serveur, de contrôle du serveur, de l'analyse à la demande et de la mise à jour de Kaspersky Security for Windows Server sont réalisées sous forme de tâches.

Ces tâches peuvent être administrées via les options du menu contextuel du nom de la tâche dans l'arborescence de la console de l'application, de la barre d'outils et de la barre d'accès rapide. Vous pouvez consulter les informations sur l'état d'une tâche dans le volet des résultats. Les opérations d'administration des tâches sont

enregistrées dans le journal d'audit système.

Il existe deux types de tâches de Kaspersky Security for Windows Server : *locales* et de *groupe*.

### Tâches locales

Les tâches locales sont uniquement exécutées sur le serveur protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- **Tâches locales du système.** Créées automatiquement lors de l'installation de Kaspersky Security for Windows Server. Vous pouvez modifier les paramètres de toutes les tâches système à l'exception des tâches Analyse de la quarantaine et Annulation de la mise à jour des bases de l'application. Il est impossible de renommer ou de supprimer les tâches système. Vous pouvez lancer les tâches d'analyse à la demande système en même temps que les tâches définies par l'utilisateur.
- **Tâches locales définies par l'utilisateur.** Vous pouvez créer des tâches d'analyse à la demande dans la console de l'application. Kaspersky Security Center permet de créer des tâches d'analyse à la demande, de mise à jour des bases de l'application, d'annulation de la mise à jour des bases de l'application 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 de groupe et les tâches pour les sélections d'ordinateurs créées via Kaspersky Security Center sont affichées dans la console de l'application. Ces tâches sont les tâches de groupe. Vous pouvez administrer les tâches de groupe et les configurer au départ de Kaspersky Security Center. La console de l'application permet uniquement de consulter l'état des tâches de groupe.

## Lancement / suspension / rétablissement / arrêt manuel des tâches

Vous ne pouvez suspendre et reprendre que les tâches Protection en temps réel du serveur et Analyse à la demande.

► *Pour lancer/suspendre/reprendre/arrêter une tâche, procédez comme suit :*

1. Ouvrez le menu contextuel de la tâche dans la console de l'application.
2. Sélectionnez une des options suivantes : **Démarrer**, **Suspendre**, **Reprendre** ou **Arrêter**.

L'opération sera effectuée et enregistrée dans le journal d'audit système (cf. page [214](#)).

Quand vous suspendez, puis relancez une tâche d'analyse à la demande, Kaspersky Security for Windows Server reprend l'analyse à l'objet qui était traité au moment de la suspension.

## Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Security for Windows Server et configurer les paramètres de la planification.

## Dans cette section

Configuration des paramètres de la planification du lancement de la tâche .....	158
Activation et désactivation du lancement programmé .....	159

## Configuration des paramètres de la planification du lancement de la tâche

La console de l'application permet de planifier le lancement des tâches locales du système et définies par l'utilisateur. Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement de la tâche, procédez comme suit :*

1. Ouvrez le menu contextuel de la tâche dont vous souhaitez configurer la planification du lancement.
2. Choisissez l'option **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la programmation**.
4. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
  - a. Choisissez une des options suivantes dans la liste **Fréquence** :
    - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
    - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
    - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s) le**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;
    - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security for Windows Server.
    - **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.
  - b. Indiquez, dans le champ **Démarrer à**, l'heure du premier lancement de la tâche.
  - c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

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, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est défini par les paramètres de la stratégie de Kaspersky Security Center.

5. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.

- Dans la section **Paramètres d'arrêt de la tâche** :
  - a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la tâche.
  - b. Cochez la case **Pause à partir de**, puis saisissez les heures de début et de fin pour spécifier un intervalle de temps de moins de 24 heures pendant lequel l'exécution de la tâche sera suspendue.
- Dans la section **Paramètres avancés** :
  - a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.
  - b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.
  - c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.

6. Cliquez sur le bouton **OK**.

La configuration des paramètres de lancement de la tâche est enregistrée.

## Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver le lancement des tâches planifiées après ou avant la configuration de la planification.

► *Pour activer ou désactiver la planification du lancement de la tâche, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nom de la tâche dont vous souhaitez planifier le lancement.
2. Choisissez l'option **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes sous l'onglet **Planification** :
  - Cochez la case **Exécuté selon la programmation** si vous souhaitez activer l'exécution planifiée d'une tâche.
  - Décochez la case **Exécuté selon la programmation** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

Les paramètres de la planification du lancement de la tâche ne sont pas supprimés. Ils sont appliqué au prochain lancement planifié de la tâche.

4. Cliquez sur le bouton **OK**.

Les paramètres configurés de la planification du lancement de la tâche sont enregistrés.

## Utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez lancer les tâches sous un compte système ou sous un autre compte utilisateur que vous désignerez.



## Dans cette section

A propos de l'utilisation des comptes utilisateur pour l'exécution des tâches .....	160
Définition du compte utilisateur pour l'exécution de la tâche.....	160

## A propos de l'utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez indiquer le compte sous les autorisations duquel vous souhaitez exécuter la tâche sélectionnée pour les modules suivants de Kaspersky Security for Windows Server :

- Tâches de Génération des règles du Contrôle des périphériques et Génération des règles du Contrôle du lancement des applications
- Tâche Analyse à la demande
- Tâches de mise à jour

Par défaut, les tâches désignées sont exécutées avec les autorisations du compte système.

Il est conseillé de définir un autre compte avec les privilèges suffisants dans les cas suivants :

- Pour la mise à jour, si la source de mise à jour est un dossier 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).
- Pour les tâches d'analyse à la demande, si le compte système ne possède pas les autorisations d'accès à un des objets à analyser (par exemple, aux fichiers dans les dossiers partagés du serveur).
- Pour la tâche de génération des règles du Contrôle du lancement des applications, si à l'issue de l'exécution de la tâche, les règles générées sont exportées vers un fichier de configuration situé dans un emplacement inaccessible au compte système (par exemple, dans un des dossiers partagés de l'ordinateur).

Vous pouvez lancer les tâches de Mise à jour, d'Analyse à la demande et de Génération des règles du Contrôle du lancement des applications avec les autorisations du compte système. Lors de l'exécution de ces tâches, Kaspersky Security for Windows Server accède aux dossiers partagés sur l'autre ordinateur du réseau si cet ordinateur est enregistré dans le même domaine que le serveur protégé. Dans ce cas, le compte système doit posséder les autorisations d'accès à ces dossiers. Kaspersky Security for Windows Server contactera cet ordinateur avec les privilèges du compte **<Nom\_de\_domaine\nom\_d'ordinateur>**.

## Définition du compte utilisateur pour l'exécution de la tâche

► *Pour sélectionner le compte utilisateur sous lequel la tâche sera exécutée, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer le lancement sous les privilèges d'un compte.
2. Choisissez l'option **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, réalisez les opérations suivantes sous l'onglet **Exécuter en tant que** :

- a. Choisissez l'option **Nom d'utilisateur**.
- b. Saisissez le nom et le mot de passe de l'utilisateur dont vous souhaitez utiliser le compte.

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

- c. Confirmez le mot de passe saisi.
4. Cliquez sur le bouton **OK**.

Les paramètres modifiés d'exécution des tâches sous les autorisations du compte utilisateur sont enregistrés.

## Importation et exportation des paramètres

Cette section aborde l'exportation des valeurs des paramètres de fonctionnement de Kaspersky Security for Windows Server ou des paramètres de fonctionnement de composants distincts de l'application dans un fichier de configuration au format XML et l'importation de ces valeurs depuis le fichier de configuration dans l'application.

### Dans cette section

A propos de l'importation et de l'exportation des paramètres .....	<a href="#">161</a>
Exportation des paramètres.....	<a href="#">163</a>
Importation des paramètres.....	<a href="#">163</a>

### A propos de l'importation et de l'exportation des paramètres

Vous pouvez exporter les paramètres de Kaspersky Security for Windows Server dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Security for Windows Server depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.

Quand vous exportez tous les paramètres de Kaspersky Security for Windows Server, le fichier reprend les paramètres généraux de l'application et les paramètres des fonctions et modules suivants de Kaspersky Security for Windows Server :

- Protection des fichiers en temps réel
- Utilisation du KSN
- Contrôle des périphériques
- Contrôle du lancement des applications
- Génération des règles du Contrôle des périphériques ;
- Génération des règles du Contrôle du lancement des applications
- Tâche d'analyse à la demande définie par l'utilisateur.
- Protection du trafic
- Monitoring des scripts

- Protection ICAP des stockages réseau connectés
- Protection RPC des stockages réseau connectés
- Protection contre le chiffrement pour NetApp
- Moniteur d'intégrité des fichiers
- Inspecteur des journaux
- Mise à jour des bases de données et des modules de l'application
- Quarantaine
- Sauvegarde
- Journaux.
- Notifications de l'administrateur et des utilisateurs
- Zone de confiance
- Protection contre les exploits
- Stockage des ordinateurs bloqués
- Protection par mot de passe

Vous pouvez également enregistrer les paramètres généraux de Kaspersky Security for Windows Server dans un fichier, avec les privilèges des comptes utilisateur.

Vous ne pouvez pas exporter les paramètres des tâches de groupe.

Kaspersky Security for Windows Server exporte tous les mots de passe qui sont utilisés par l'application, par exemple, les données des comptes d'exécution des tâches ou de connexion au serveur proxy. Les mots de passe exportés dans le fichier de configuration sont chiffrés. Vous pouvez importer les mots de passe uniquement à l'aide d'une version de Kaspersky Security for Windows Server installée sur ce serveur, si elle n'a pas été réinstallée ou mise à jour.

Vous ne pouvez pas importer des mots de passe préalablement enregistrés à l'aide d'une version de Kaspersky Security for Windows Server installée sur un autre ordinateur. Après l'importation des paramètres sur un autre ordinateur, vous devrez saisir tous les mots de passe manuellement.

Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, l'application exporte les valeurs appliquées par la stratégie.

Vous pouvez importer les paramètres depuis le fichier de configuration qui contient les paramètres uniquement de certains composants de Kaspersky Security for Windows Server (par exemple, créé dans une version de Kaspersky Security for Windows Server sans la totalité des composants). Après l'importation des paramètres, seuls les paramètres de Kaspersky Security for Windows Server repris dans le fichier de configuration sont modifiés. Les autres paramètres demeurent inchangés.

**Les paramètres verrouillés de la stratégie active de Kaspersky Security Center ne sont pas modifiés lors de l'importation des paramètres.**

## Exportation des paramètres

► *Pour exporter les paramètres dans un fichier de configuration, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, réalisez une des opérations suivantes :
  - Dans le menu contextuel du nœud **Kaspersky Security**, sélectionnez **Exporter les paramètres** pour exporter tous les paramètres de Kaspersky Security for Windows Server.
  - Dans le menu contextuel du nom de la tâche dont vous souhaitez exporter les paramètres, choisissez l'option **Exporter les paramètres** afin d'exporter les paramètres d'un module individuel de l'application.
  - Pour exporter les paramètres du composant Zone de confiance :
    - a. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
    - b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.  
La fenêtre **Zone de confiance** s'ouvre.
    - c. Cliquez sur le bouton **Exporter**.  
La fenêtre de bienvenue de l'Assistant d'exportation des paramètres s'ouvre.
2. 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.  
Pour désigner le chemin d'accès, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, l'application exporte les valeurs des paramètres de la stratégie.

3. Dans la fenêtre **Exportation des paramètres de l'application terminée**, cliquez sur le bouton **Fermer**.  
L'Assistant d'exportation des paramètres se ferme et l'exportation des paramètres sera terminée.

## Importation des paramètres

► *Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, réalisez une des opérations suivantes :
  - Dans le menu contextuel du nœud **Kaspersky Security**, sélectionnez **Importer les paramètres** pour importer tous les paramètres de Kaspersky Security for Windows Server.
  - Dans le menu contextuel du nom de la tâche dont vous souhaitez importer les paramètres, choisissez l'option **Importer les paramètres**, afin d'importer les paramètres d'un module individuel de l'application.
  - Pour importer les paramètres du composant Zone de confiance :
    - a. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
    - b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.  
La fenêtre **Zone de confiance** s'ouvre.

- c. Cliquez sur **Importer**.

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.

Une fois que les paramètres généraux de Kaspersky Security for Windows Server et de ses composants auront été importés sur le serveur, vous ne pourrez plus revenir à leurs valeurs antérieures.

3. Dans la fenêtre **Importation des paramètres de l'application terminée**, cliquez sur le bouton **Fermer**.  
L'Assistant d'importation des paramètres se ferme ; les paramètres importés sont enregistrés.
4. Cliquez sur le bouton **Actualiser** dans la barre d'outils de la console de l'application.  
Les paramètres importés apparaissent dans la fenêtre de la console de l'application.

Kaspersky Security for Windows Server n'importe pas les mots de passe (identifiants pour l'exécution de tâches ou la connexion au serveur proxy) d'un fichier créé sur un autre serveur ou sur ce même serveur après une réinstallation ou de mise à jour de Kaspersky Security for Windows Server sur celui-ci. Après la fin de l'importation, vous devrez saisir les mots de passe manuellement.

## Utilisation des modèles de paramètres de sécurité

Cette section explique l'utilisation des modèles de paramètres de sécurité dans les tâches de protection et d'analyse de Kaspersky Security for Windows Server.

### Dans cette section

A propos des modèles de paramètres de sécurité .....	<a href="#">164</a>
Création d'un modèle de paramètres de sécurité .....	<a href="#">165</a>
Consultation des paramètres de sécurité du modèle .....	<a href="#">165</a>
Application du modèle de paramètres de sécurité .....	<a href="#">166</a>
Suppression du modèle de paramètres de sécurité .....	<a href="#">167</a>

### A propos des modèles de paramètres de sécurité

Vous pouvez configurer manuellement les paramètres de sécurité du nœud dans l'arborescence des ressources fichier du serveur et enregistrer les valeurs définies dans un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Security for Windows Server.

L'utilisation de modèles est accessible lors de la configuration des paramètres de sécurité des tâches suivantes de Kaspersky Security for Windows Server :

- Protection des fichiers en temps réel
- Protection RPC des stockages réseau connectés
- Analyse au démarrage du système d'exploitation
- Analyse des zones critiques
- Tâche d'analyse à la demande définie par l'utilisateur.

Les paramètres de sécurité d'un modèle appliqué à un nœud parent dans l'arborescence des ressources de fichier de l'ordinateur sont appliqués à tous les nœuds enfants. Le modèle d'un nœud parent n'est pas appliqué aux nœuds enfants dans les cas suivants :

- Si les paramètres de sécurité des nœuds enfants ont été configurés séparément (cf. section "Application du modèle de paramètres de sécurité" à la page [166](#)).
- Si les nœuds enfants sont virtuels. Il faudra alors appliquer le modèle pour chaque nœud virtuel séparément.

## Création d'un modèle de paramètres de sécurité

► *Pour enregistrer manuellement les paramètres de sécurité du nœud et les enregistrer dans le modèle, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez consulter le modèle de sécurité.
2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources de fichier réseau du serveur, sélectionnez le modèle que vous souhaitez consulter.
4. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Enregistrer comme modèle**.  
La fenêtre **Propriétés du modèle** s'ouvre.
5. Dans le champ **Nom du modèle**, saisissez le nom du modèle.
6. Dans le champ **Description**, saisissez toute information complémentaire relative au modèle.
7. Cliquez sur le bouton **OK**.

Le modèle avec la sélection de paramètres de sécurité sera conservé.

## Consultation des paramètres de sécurité du modèle

► *Pour consulter les valeurs des paramètres de sécurité dans le modèle créé, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche dont vous souhaitez consulter le modèle de sécurité.
2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.  
La fenêtre **Modèles** s'ouvre.
3. Dans la liste des modèles de la fenêtre qui s'ouvre, sélectionnez le modèle que vous souhaitez consulter.
4. Cliquez sur le bouton **Voir**.

La fenêtre **<Nom du modèle>** s'ouvre. L'onglet **Général** reprend les noms des modèles et les informations

complémentaires sur le modèle ; l'onglet **Options** reprend la liste des valeurs des paramètres de sécurité enregistrés dans le modèle.

## Application du modèle de paramètres de sécurité

► *Pour appliquer les modèles de sécurité du modèle au nœud sélectionné, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez consulter le modèle de sécurité.
2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources de fichier réseau du serveur, ouvrez le menu contextuel du nœud ou de l'élément auquel vous souhaitez appliquer le modèle.
4. Sélectionnez **Appliquer un modèle** → **<Nom du modèle>**.
5. Cliquez sur le bouton **Enregistrer**.

Le modèle de paramètres de sécurité est appliqué au nœud sélectionné dans l'arborescence des ressources de fichier du serveur. Sous l'onglet **Niveau de sécurité** du nœud sélectionné, la valeur **Personnalisé** apparaît.

Les valeurs des paramètres de sécurité du modèle appliqué à un nœud parent dans l'arborescence des ressources de fichiers du serveur sont appliquées à tous les nœuds enfants.

Si la zone de protection ou zone d'analyse des nœuds enfants dans l'arborescence des ressources de fichiers du serveur a été configurée séparément, les paramètres de sécurité du modèle appliqué au nœud parent ne sont pas appliqués automatiquement aux nœuds enfants.

► *Pour définir les paramètres de sécurité du modèle pour toutes les sous-entrées, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez consulter le modèle de sécurité.
2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources de fichier réseau du serveur, choisissez un nœud parent pour appliquer le modèle à ce nœud et à tous les nœud enfant.
4. Dans le menu contextuel, sélectionnez **Appliquer un modèle** → **<Nom du modèle>**.
5. Cliquez sur le bouton **Enregistrer**.

Le modèle de paramètres de sécurité est appliqué au parent et à tous les nœuds enfants dans l'arborescence des ressources de fichier du serveur. Sous l'onglet **Niveau de sécurité** du nœud sélectionné, la valeur **Personnalisé** apparaît.



## Suppression du modèle de paramètres de sécurité

► *Pour supprimer un modèle de paramètres de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour la configuration de laquelle vous ne souhaitez plus utiliser un modèle de paramètres de sécurité.
2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

Vous pouvez consulter les modèles de paramètres pour les tâches d'analyse à la demande depuis le panneau de détails du nœud principal **Analyse à la demande**.

La fenêtre **Modèles** s'ouvre.

3. Dans la liste des modèles de la fenêtre qui s'ouvre, sélectionnez le modèle que vous souhaitez supprimer.
4. Cliquez sur le bouton **Supprimer**.

La fenêtre de confirmation de la suppression s'ouvre.

5. Cliquez sur **Oui** dans la fenêtre qui s'ouvre.

Le modèle sélectionné sera supprimé.

Si le modèle de paramètres de sécurité a été appliqué à la protection ou à l'analyse d'entrées des ressources de fichier du serveur, les paramètres de sécurité configurés pour ces entrées sont conservés après la suppression du modèle.

## Consultation de l'état de la protection et des informations de Kaspersky Security for Windows Server

► *Pour lire les informations relatives à l'état de la protection du serveur dans Kaspersky Security for Windows Server,*

Sélectionnez le nœud **Kaspersky Security** dans l'arborescence de la Console de l'application.

Par défaut, les informations du panneau de détails de la console de l'application sont automatiquement actualisées :

- Toutes les 10 secondes en cas de connexion locale.
- Toutes les 15 secondes en cas de connexion distante.

Vous pouvez actualiser les informations manuellement.

► *Pour actualiser manuellement les informations du nœud **Kaspersky Security**,*

choisissez l'option **Actualiser** dans le menu contextuel du nœud **Kaspersky Security**.

Le panneau de détails de la console de l'application affiche les informations suivantes sur la console de l'application :

- Etat d'utilisation de Kaspersky Security Network.

- Etat de la protection du serveur.
- Données sur la mise à jour des bases de données et des modules de l'application.
- Données de diagnostic réel.
- Données relatives aux tâches de contrôle du serveur.
- Informations relatives à la licence.
- Etat de l'intégration à Kaspersky Security Center : données de l'ordinateur doté de Kaspersky Security Center auquel l'application est connectée ; informations sur les tâches de l'application contrôlées par la stratégie active.

Différentes couleurs sont utilisées pour indiquer l'état de la protection :

- *Vert*. La tâche est exécutée conformément aux paramètres définis. La protection est active.
- *Jaune*. La tâche n'a pas été lancée, a été suspendue ou est arrêtée. Des menaces pour la sécurité peuvent apparaître. Il est conseillé de lancer la tâche.
- *Rouge*. La tâche s'est soldée sur une erreur ou une menace pour la sécurité a été détectée pendant l'exécution de la tâche. Il est conseillé de lancer la tâche ou d'adopter les mesures d'élimination de la menace détectée.

Une partie des informations du groupe (par exemple, les noms des tâches ou le nombre de menaces détectées) se présente sous la forme de liens qui permettent d'accéder au nœud de la tâche correspondante ou d'ouvrir le journal d'exécution de la tâche.

La section **Utilisation du Kaspersky Security Network** indique l'état actuel de la tâche (par exemple, *Exécution en cours*, *Stoppée* ou *Jamais exécutée*). L'indicateur peut prendre les valeurs suivantes :

- *Verte* : la tâche Utilisation du KSN est en cours d'exécution et les demandes d'états des URL sont en cours d'envoi à KSN.
- *Jaune* : une des déclarations est acceptée mais la tâche n'est pas en cours d'exécution ou les demandes d'états des URL ne sont pas envoyées à KSN.

## Protection du serveur

La section **Protection du serveur** (cf. tableau ci-après) affiche les informations sur l'état actuel de la protection du serveur.

Tableau 27. Informations sur l'état de la protection du serveur

Section Protection	Informations
<b>Indicateur d'état de la protection du serveur</b>	<p>La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• <i>Verte</i> : cette couleur s'affiche par défaut et indique que le composant Protection des fichiers en temps réel est installé et que la tâche est en cours d'exécution.</li> <li>• <i>Jaune</i> : le composant Protection des fichiers en temps réel n'est pas installé et la tâche Analyse des zones critiques n'a pas été exécutée depuis longtemps.</li> <li>• <i>Rouge</i> : la tâche de protection des fichiers en temps réel n'est pas en cours d'exécution.</li> </ul>

Section Protection	Informations
<b>Protection des fichiers en temps réel</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Déecté</b> : nombre d'objets détectés par Kaspersky Security for Windows Server. Par exemple, si Kaspersky Security for Windows Server a découvert une application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité. Si le nombre d'applications malveillantes détectées dépasse 0, la valeur est mise en évidence en rouge.</p>
<b>Analyse des zones critiques</b>	<p><b>Date de la dernière analyse</b> : date et heure de la dernière analyse rapide à la recherche de virus et autres menaces informatiques.</p> <p><i>Jamais exécutée</i> : événement qui survient quand la tâche Analyse des zones critiques a été effectuée il y a 30 jours ou plus (par défaut). Vous pouvez modifier le seuil de déclenchement de l'événement.</p>
<b>Protection du trafic</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Plug-in Outlook</b> : installé ou pas.</p>
<b>Protection contre les exploits</b>	<p><b>Etat</b> : état actuel des techniques de protection contre les exploits, par exemple <i>Appliqué</i> ou <i>Pas appliquée</i>.</p> <p><b>Mode de prévention</b> : un des deux modes à sélectionner lors de la configuration de la protection de la mémoire des processus.</p> <ul style="list-style-type: none"> <li>• Terminer en cas d'exploit.</li> <li>• Statistiques uniquement.</li> </ul> <p><b>Processus protégés</b> : total des processus ajoutés à la zone de protection et traités selon le mode sélectionné.</p>
<b>Objets sauvegardés</b>	<p><i>Dépassement du seuil d'espace disponible dans la Sauvegarde</i> : cet événement qui produit si la quantité d'espace disponible dans la Sauvegarde approche la limite indiquée. Kaspersky Security for Windows Server poursuit la mise en sauvegarde des objets. Dans ce cas, la valeur du champ <b>Espace utilisé</b> est mise en évidence en jaune.</p> <p><i>Dépassement de la taille maximum de Sauvegarde</i> : cet événement se produit si la taille de la Sauvegarde a atteint la limite indiquée. Kaspersky Security for Windows Server poursuit la mise en sauvegarde des objets. Dans ce cas, la valeur du champ <b>Espace utilisé</b> est mise en évidence en rouge.</p> <p><b>Objets sauvegardés</b> : nombre d'objets présents actuellement dans la Sauvegarde.</p> <p><b>Espace utilisé</b> : volume d'espace occupé dans la Sauvegarde.</p>

### Mise à jour

La section **Mise à jour** (cf. tableau ci-dessous) affiche les informations sur l'actualité des bases antivirus et des modules de l'application.

Tableau 28. Informations sur l'état des bases et des modules de Kaspersky Security for Windows Server

Section Mise à jour	Informations
<b>Témoin de l'état des bases et des modules de l'application</b>	<p>La couleur du panneau portant le nom de la section indique l'état des bases de l'application et des modules. L'indicateur peut prendre les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• Verte : cette couleur s'affiche par défaut et indique que les bases de l'application sont à jour et que la dernière tâche de mise à jour des bases de l'application a été effectuée avec succès.</li> <li>• Jaune : les bases de données sont dépassées ou la dernière tâche de mise à jour des bases de l'application a échoué.</li> <li>• Rouge : l'événement <i>Les bases de l'application sont fortement dépassées</i> ou <i>Bases de l'application endommagées</i> s'est produit.</li> </ul>
<b>Mise à jour des bases de l'application et Mise à jour des modules de l'application</b>	<p><b>Etat des bases de l'application</b> : évaluation de l'état de la tâche de mise à jour des bases de l'application.</p> <p>Le paramètre peut prendre les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• <b>Bases de l'application à jour</b> : les bases de l'application ont été mises à jour il y a 7 jours maximum (par défaut).</li> <li>• <b>Les bases de l'application sont dépassées</b> : les bases de l'application ont été mises à jour il y a 7 à 14 jours (par défaut).</li> <li>• <b>Les bases de l'application sont fortement dépassées</b> : les bases de l'application ont été mises à jour il y a plus de 14 jours (par défaut).</li> </ul> <p>Vous pouvez modifier les seuils de déclenchement des événements <i>Les bases de l'application sont dépassées</i> et <i>Les bases de l'application sont fortement dépassées</i>.</p> <p><b>Date de publication des bases de l'application</b> : date et heure de la publication de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées en TU.</p> <p><b>Etat de la tâche Mise à jour des bases de l'application la plus récente</b> : date et heure de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées selon l'heure locale du serveur à protéger. Le champ est rouge si l'événement <i>Echec</i> s'est produit.</p> <p><b>Nombre de mises à jour des modules disponibles</b> : nombre de mises à jour des modules de Kaspersky Security for Windows Server prêtes à être téléchargées et installées.</p> <p><b>Nombre de mises à jour des modules installées</b> : nombre de mises à jour des modules de Kaspersky Security for Windows Server installées.</p>

### Contrôle

La section **Contrôle** (cf. tableau ci-dessous) affiche les informations sur l'état des tâches Contrôle du lancement des applications, Contrôle des périphériques, Protection contre le chiffrement et Gestion du pare-feu.

Tableau 29. Informations sur l'état du contrôle du serveur

Section Contrôle	Informations
<b>Indicateur d'état du contrôle du serveur</b>	<p>La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• Vert : cette couleur s'affiche par défaut et indique que le composant Contrôle du lancement des applications est installé et que la tâche s'exécute en mode actif ;</li> <li>• Jaune : le contrôle du lancement des applications est en cours d'exécution en mode Statistiques uniquement.</li> <li>• Rouge : la tâche Contrôle du lancement des applications est à l'arrêt ou a échoué.</li> </ul>
<b>Contrôle du lancement des applications</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Mode</b> : un des deux modes disponibles pour la tâche Contrôle du lancement des applications :</p> <ul style="list-style-type: none"> <li>• Actif</li> <li>• Statistiques uniquement</li> </ul> <p><b>Lancements des applications bloqués</b> : nombre de tentatives de lancement d'applications bloquées par Kaspersky Security for Windows Server au cours de l'exécution de la tâche Contrôle du lancement des applications. Si le nombre de lancements d'applications bloquées dépasse 0, le champ est rouge.</p> <p><b>Durée de traitement moyenne (en ms)</b> : temps nécessaire à Kaspersky Security for Windows Server pour le traitement des tentatives de lancement d'applications sur le serveur protégé.</p>
<b>Contrôle des périphériques</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Mode</b> : un des deux modes disponibles pour la tâche Contrôle des périphériques :</p> <ul style="list-style-type: none"> <li>• <b>Actif</b></li> <li>• <b>Statistiques uniquement</b></li> </ul> <p><b>Appareils bloqués</b> : nombre de tentatives de connexion à un périphérique de stockage de masse bloquées par Kaspersky Security for Windows Server au cours de l'exécution de la tâche Contrôle des périphériques. Si le nombre de stockages de masse bloqués dépasse 0, le champ est rouge.</p>
<b>Protection contre le chiffrement</b>	<p>Etat de la tâche : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p>Mode de fonctionnement : un des deux modes disponibles pour la tâche Protection contre le chiffrement.</p> <ul style="list-style-type: none"> <li>• <b>Actif</b></li> <li>• <b>Statistiques uniquement</b></li> </ul> <p><b>Hôtes bloqués</b> : nombre d'hôtes qui ont affiché une activité malveillante et qui ont été bloqués lors de la tentative de connexion au serveur protégé.</p>
<b>Gestion du pare-feu</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Tentatives de connexion bloquées</b> : nombre de connexions à un serveur protégé qui ont été bloquées par les règles du pare-feu définies.</p>

## Diagnostic

La section **Diagnostic** (cf. tableau ci-après) affiche les informations relatives à l'état des tâches Moniteur d'intégrité des fichiers et Inspection des journaux.

Tableau 30. Informations sur l'état du diagnostic du système

Section Diagnostic	Informations
<b>Indicateur d'état du diagnostic</b>	<p>La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• Vert : cette couleur s'affiche par défaut et indique qu'un des composants de diagnostic du système ou les deux sont installés et que des tâches sont en cours d'exécution.</li> <li>• Jaune : les deux composants sont installés mais une des tâches de diagnostic du système n'est pas en cours d'exécution ; l'événement <i>A l'arrêt</i> se produit.</li> <li>• Rouge : une des tâches a échoué.</li> </ul>
<b>Moniteur d'intégrité des fichiers</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Opérations sur les fichiers non autorisées</b> : nombre de modifications dans les fichiers au sein de la zone de monitoring. Ces modifications peuvent signaler une violation de la sécurité d'un serveur protégé.</p>
<b>Inspection des journaux</b>	<p><b>Etat de la tâche</b> : état actuel de la tâche (par exemple, <i>Exécution en cours</i> ou <i>Arrêtée</i>).</p> <p><b>Violations potentielles</b> : nombre de violations enregistrées d'après les données du journal des événements Windows. Ce nombre est déterminé sur la base des règles définies de la tâche ou via l'analyseur heuristique</p>

Les informations relatives à la licence de Kaspersky Security for Windows Server sont affichées sur la ligne du coin inférieur gauche du panneau de détails du nœud **Kaspersky Security**.

Vous pouvez configurer les propriétés de Kaspersky Security for Windows Server en suivant le lien **Propriétés de l'application** (cf. section "Paramètres de Kaspersky Security for Windows Server dans la Console de l'application" à la page [143](#)).

Vous pouvez établir une connexion sur un autre ordinateur via le lien **Se connecter à un autre ordinateur** (voir la section "Administration de Kaspersky Security for Windows Server via la Console de l'application sur un autre ordinateur" à la page [156](#)).

Pour en savoir plus sur l'onglet Protection des stockages réseau, consultez le Manuel d'implantation de la protection des stockages réseau de Kaspersky Security for Windows Server.

## Interface de diagnostic compacte

Cette section explique comment utiliser l'interface de diagnostic compacte pour réviser l'état du serveur ou l'activité en cours et comment configurer l'écriture de fichiers dump et de fichiers de trace.

### Contenu du chapitre

A propos de l'interface de diagnostic compacte .....	<a href="#">173</a>
Révision de l'état de Kaspersky Security for Windows Server via l'interface de diagnostic compacte .....	<a href="#">174</a>
Révision des statistiques des événements de sécurité .....	<a href="#">175</a>
Révision de l'activité en cours de l'application.....	<a href="#">175</a>
Configuration de l'écriture de fichiers dump et de fichiers de trace.....	<a href="#">176</a>

## A propos de l'interface de diagnostic compacte

Le composant Interface de diagnostic compacte (également appelé "CDI") est installé et désinstallé avec le composant Icône dans la barre d'état système indépendamment de la console de l'application et peut être utilisé quand la console de l'application n'est pas installée sur le serveur protégé. Le composant CDI est lancé depuis l'icône de la barre d'état système ou via l'exécution du fichier kavfsmui.exe depuis le dossier de l'application sur le serveur.

La fenêtre de la CDI permet de réaliser les opérations suivantes :

- Consultation des informations sur l'état général de l'application (cf. section "Révision de l'état de Kaspersky Security for Windows Server via l'interface de diagnostic compacte" à la page [174](#)).
- Réviser les incidents de sécurité qui se sont produits (cf. section "Révision des statistiques des événements de sécurité" à la page [175](#)).
- Réviser l'activité en cours sur le serveur protégé (cf. section "Révision de l'activité en cours de l'application" à la page [175](#)).
- Lancez ou arrêtez l'écriture des fichiers dump et de fichiers de trace (cf. section "Configuration de l'écriture de fichiers dump et de fichiers de trace" à la page [176](#)).
- Ouvrez la console de l'application.
- Ouvrez la fenêtre **A propos de l'application** qui reprend la liste des mises à jour et des correctifs disponibles.

Le CDI est disponible même si l'accès à la fonction de Kaspersky Security for Windows Server est protégés par un mot de passe. Aucun mot de passe requis.

Le composant CDI ne peut pas être configuré via Kaspersky Security Center.



## Révision de l'état de Kaspersky Security for Windows Server via l'interface de diagnostic compacte

► Pour ouvrir la fenêtre *Interface de diagnostic compacte*, procédez comme suit :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Security for Windows Server dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.

La fenêtre **Interface de diagnostic compacte** s'affiche.

Consultez l'état actuel de la clé, des tâches Protection en temps réel du serveur et des tâches de mise à jour sous l'onglet **Etat de la protection**. Différentes couleurs sont utilisées pour avertir l'utilisateur sur l'état de la protection (cf. tableau ci-dessous).

Tableau 31. Etat de protection de l'interface de diagnostic compacte

Section	Etat
<b>Protection en temps réel du serveur</b>	<p>Le panneau est <i>vert</i> pour les scénarios suivants (un nombre quelconque des conditions est rempli) :</p> <ul style="list-style-type: none"> <li>• Configuration recommandée : <ul style="list-style-type: none"> <li>• La tâche Protection des fichiers en temps réel est démarrée selon les paramètres par défaut.</li> <li>• La tâche Contrôle du lancement des applications est démarrée en mode <b>Actif</b> avec les paramètres par défaut.</li> </ul> </li> <li>• Configuration acceptable : <ul style="list-style-type: none"> <li>• La tâche Protection des fichiers en temps réel est configurée par l'utilisateur.</li> <li>• Les paramètres de la tâche Contrôle du lancement des applications sont modifiés.</li> </ul> </li> </ul>
	<p>Le panneau est <i>jaune</i> si une ou plusieurs des conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• La tâche Protection des fichiers en temps réel est suspendue (par l'utilisateur ou selon une programmation).</li> <li>• La tâche Contrôle du lancement des applications est démarrée en mode <b>Statistiques uniquement</b>.</li> <li>• Protection contre les exploits et Contrôle du lancement des applications sont démarrés en mode <b>Statistiques uniquement</b>.</li> </ul>
	<p>Le panneau est <i>rouge</i> si une ou plusieurs des conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Le composant Protection des fichiers en temps réel n'est pas installé ou la tâche est arrêtée ou suspendue.</li> <li>• Le composant Contrôle du lancement des applications n'est pas installé ou la tâche Contrôle du lancement des applications est démarrée en mode <b>Statistiques uniquement</b>.</li> </ul>
<b>Licence</b>	Le panneau est <i>vert</i> si la licence en cours est valide.

	<p>Un panneau <i>jaune</i> indique qu'un des événements suivants s'est produit :</p> <ul style="list-style-type: none"> <li>• <b>Vérification de l'état de la licence.</b></li> <li>• <b>Il reste 14 jours avant l'expiration de la licence et aucune clé additionnelle ou code d'activation n'a été ajouté.</b></li> <li>• <b>La clé ajoutée est inscrite sur la liste noire et va bientôt être bloquée.</b></li> </ul>
	<p>Un panneau <i>rouge</i> indique qu'un des événements suivants s'est produit :</p> <ul style="list-style-type: none"> <li>• <b>L'application n'a pas été activée.</b></li> <li>• <b>Licence expirée</b></li> <li>• <b>Violation du Contrat de licence utilisateur final</b></li> <li>• <b>Clé placée dans la liste noire</b></li> </ul>
<b>Mise à jour</b>	Le panneau est <i>vert</i> lorsque les bases de l'application sont à jour.
	Le panneau est <i>jaune</i> lorsque les bases de l'application sont dépassées.
	Le panneau est <i>rouge</i> lorsque les bases de l'application sont fortement dépassées.

## Révision des statistiques des événements de sécurité

L'onglet **Statistiques** affiche tous les événements de sécurité. Les statistiques de chaque tâche de protection s'affichent dans un bloc séparé, spécifiant le nombre d'incidents, ainsi que la date et l'heure de survenue du dernier incident. Lorsqu'un incident est enregistré, le bloc devient rouge.

► *Pour consulter les statistiques :*

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Security for Windows Server dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.  
La fenêtre **Interface de diagnostic compacte** s'affiche.
3. Ouvrez l'onglet **Statistiques**.
4. Révisez les incidents de sécurité pour les tâches de protection.

## Révision de l'activité en cours de l'application

Cet onglet permet de consulter l'état des tâches et des processus en cours de l'application et d'obtenir des notifications rapides sur les événements critiques qui se produisent.

Différentes couleurs sont utilisées pour indiquer l'état de l'activité de l'application :

- Dans la section **Tâches** :
  - *Vert*. Aucune condition pour un état jaune ou rouge.
  - *Jaune*. Analyse des zones critiques non réalisée depuis longtemps.
  - *Rouge*. N'importe laquelle des conditions suivantes est vraie :
    - Aucune tâche n'est lancée et la planification du lancement n'est défini pour aucune des tâches.

- Les erreurs de lancement de l'application sont consignées en tant qu'événements critiques.
- Dans la section **Kaspersky Security Network** :
  - *Vert*. La tâche Utilisation du KSN est lancée.
  - *Jaune*. La Déclaration de KSN est acceptée, mais la tâche n'est pas lancée.

► *Pour consulter l'activité en cours de l'application sur le serveur :*

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Security for Windows Server dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.  
La fenêtre **Interface de diagnostic compacte** s'affiche.
3. Ouvrez l'onglet **Activité actuelle de l'application**.
4. Consultez les informations suivantes dans la section **Tâches** :

- **Les zones critiques n'ont pas été analysées depuis longtemps**

Ce champ est affiché uniquement si l'application renvoie un avertissement correspondants sur les analyses des zones critiques.

- **En cours d'exécution**
  - **Echec de l'exécution**
  - **Prochain lancement planifié**
5. Consultez les informations suivantes dans la section **Kaspersky Security Network** :
    - **KSN est activé. Les services concernant la réputation des fichiers sont activés** ou la **protection est désactivée**.
    - **Statistiques de l'application envoyées à KSN.**  
L'application envoie les données sur les détections d'applications malveillantes, y compris les logiciels frauduleux détectés pendant l'exécution des tâches de protection des fichiers en temps réel et d'analyse à la demande, ainsi que les informations de débogage relatives aux échecs survenus lors de l'analyse.  
Ce champ apparaît quand la case **Envoyer les statistiques de Kaspersky Security Network** est sélectionnée dans les paramètres de la tâche Utilisation du KSN.
  6. Consultez les informations suivantes dans la section **Intégration à Kaspersky Security Center** :
    - L'administration locale est autorisée.
    - La stratégie est appliquée : <nom du serveur Kaspersky Security Center>.

## Configuration de l'écriture de fichiers dump et de fichiers de trace

Vous pouvez configurer l'écriture de fichiers dump et de fichiers de trace via la CDI.

Vous pouvez également configurer les diagnostics de dysfonctionnement via la Console de l'application (cf. section "Paramètres de Kaspersky Security for Windows Server dans la Console de l'application" à la page [143](#)).

► Pour commencer à écrire les fichiers dump et de trace, réaliser les opérations suivantes :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Security for Windows Server dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.  
La fenêtre **Interface de diagnostic compacte** s'affiche.
3. Ouvrez l'onglet **Dépannage**.
4. Le cas échéant, configurez les paramètres suivants de la trace :
  - a. Cochez la case **Ecrivez les informations de débogage dans le fichier de trace dans ce dossier**.
  - b. Cliquez sur le bouton **Parcourir** afin de désigner le dossier où Kaspersky Security for Windows Server va enregistrer les fichiers de trace.  
Le traçage sera activé pour tous les composants avec les paramètres par défaut avec le niveau de détail **Débogage** et la taille de journal maximale par défaut de 50 Mo.
5. Le cas échéant, configurez les paramètres suivants des fichiers dump :
  - a. Cochez la case **Créez un fichier dump dans ce dossier en cas de dysfonctionnement**.
  - b. Cliquez sur le bouton **Parcourir** afin de désigner le dossier où Kaspersky Security for Windows Server va enregistrer les fichiers dump.
6. Cliquez sur le bouton **Appliquer**.  
Une nouvelle configuration est appliquée.

# Mise à jour des bases de données et des modules de l'application Kaspersky Security for Windows Server

Cette section présente les tâches de mises à jour des bases de données et des modules de l'application Kaspersky Security for Windows Server, la copie des mises à jour des bases de données et le retour à l'état antérieur aux mises à jour. Elle explique également comment configurer les paramètres des tâches de mise à jour des bases de données et des modules de l'application.

## Contenu du chapitre

A propos des tâches de mise à jour .....	<a href="#">178</a>
A propos de la mise à jour des modules de l'application Kaspersky Security for Windows Server .....	<a href="#">179</a>
A propos des mises à jour des bases de l'application Kaspersky Security for Windows Server .....	<a href="#">180</a>
Schémas de mise à jour des bases et des modules des applications antivirus dans l'entreprise .....	<a href="#">180</a>
Configuration des tâches de mise à jour .....	<a href="#">184</a>
Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server .....	<a href="#">190</a>
Remise à l'état antérieur à la mise à jour des modules de l'application .....	<a href="#">191</a>
Statistiques sur les tâches de mise à jour .....	<a href="#">191</a>

## A propos des tâches de mise à jour

Kaspersky Security for Windows Server fournit quatre tâches de mise à jour du système : Mise à jour des bases de l'application, Mise à jour des modules de l'application, Copie des mises à jour et Annulation de la mise à jour des bases de l'application.

Par défaut Kaspersky Security for Windows Server établit la connexion à la source des mises à jour (un des ordinateurs de mise à jour de Kaspersky Lab) toutes les heures. Vous pouvez configurer toutes les tâches de mises à jour (cf. section "Configuration des tâches de mise à jour" à la page [184](#)), à l'exception de la tâche Annulation de la mise à jour des bases de l'application. Une fois que les paramètres de la tâche ont été modifiés, Kaspersky Security for Windows Server appliquera les nouvelles valeurs au prochain lancement de l'application.

Vous ne pouvez pas suspendre et reprendre une tâche de mise à jour.

### Mise à jour des bases de l'application

Par défaut, Kaspersky Security for Windows Server copie les bases depuis la source de mise à jour sur le serveur protégé et les utilise directement dans la tâche Protection en temps réel du serveur en cours. Les tâches Analyse à la demande utiliseront les bases de l'application mises à jour à leur prochaine exécution.

Par défaut, Kaspersky Security for Windows Server lance la tâche Mise à jour des bases de l'application toutes les heures.

### Mise à jour des modules de l'application

Par défaut, Kaspersky Security for Windows Server vérifie la disponibilité des mises à jour des modules de l'application sur la source de mise à jour. L'utilisation des modules de l'application installés exige le redémarrage de

l'ordinateur et/ou le de Kaspersky Security for Windows Server.

Par défaut, Kaspersky Security for Windows Server lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé). Pendant l'exécution de la tâche, l'application recherche la présence éventuelle de mises à jour prévues ou extraordinaires pour les modules de Kaspersky Security for Windows Server, mais ne les distribue pas.

### Copie des mises à jour

Par défaut, lors de l'exécution de la tâche, Kaspersky Security for Windows Server télécharge les fichiers de mise à jour des bases de l'application et les enregistre dans le dossier de réseau ou dans le dossier local indiqué, sans les appliquer.

La Copie des mises à jour n'est pas exécutée par défaut.

### Annulation de la mise à jour des bases de l'application

Au cours de cette tâche, Kaspersky Security for Windows Server utilise à nouveau les bases de la mise à jour antérieure.

La tâche Annulation de la mise à jour des bases de l'application n'est pas exécutée par défaut.

## A propos de la mise à jour des modules de l'application Kaspersky Security for Windows Server

Kaspersky Lab peut diffuser des paquets de mise à jour pour les modules de Kaspersky Security for Windows Server. Les mises à jour sont réparties entre les *mises à jour urgentes* (ou *critiques*) et les mises à jour prévues. Les mises à jour critiques suppriment des vulnérabilités et corrigent les erreurs tandis que les mises à jour prévues peuvent ajouter de nouvelles fonctions ou améliorer des fonctions existantes.

Les mises à jour urgentes (critiques) sont publiées sur les serveurs de mise à jour de Kaspersky Lab. Vous pouvez configurer l'installation automatique grâce à la tâche Mise à jour des modules de l'application. Par défaut, Kaspersky Security for Windows Server lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour 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 Security for Windows Server à l'aide la tâche Mises à jour des modules de l'application.

Vous pouvez télécharger les mises à jour critiques 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 les diffuser sur les serveurs du réseau. Pour copier et enregistrer les mises à jour sans les installer, utilisez la tâche Copie des mises à jour.

Avant d'installer les mises à jour des modules, Kaspersky Security for Windows Server crée une copie de sauvegarde des modules installés antérieurement. Si la mise à jour des modules de l'application est interrompue ou si elle se solde par un échec, Kaspersky Security for Windows Server utilisera à nouveau automatiquement les modules installés précédemment. Vous pouvez aussi décider de revenir manuellement à l'état antérieur à la mise à jour des modules.

Lors de l'installation des mises à jour récupérées, le Service Kaspersky Security s'arrête puis redémarre automatiquement.

## A propos des mises à jour des bases de l'application Kaspersky Security for Windows Server

Les bases de Kaspersky Security for Windows Server 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 de l'application. Une Mise à jour des bases de données est un fichier ou un ensemble de fichiers 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 de l'ordinateur au minimum, il est conseillé de réaliser une mise à jour régulière des bases de données.

Par défaut, si les bases de données de Kaspersky Security for Windows Server n'ont pas été mises à jour dans la semaine qui suit la création de la dernière mise à jour des bases de données installée, l'événement *Les bases de l'application sont dépassées* est déclenché. Si les bases de données restent deux semaines sans mises à jour, l'événement *Les bases de l'application sont fortement dépassées* est déclenché. Les informations relatives à l'état de mise à jour des bases de données (cf. section "Consultation de l'état de la protection et des informations de Kaspersky Security for Windows Server" à la page [167](#)) sont affichées dans le nœud **Kaspersky Security** de l'arborescence de la console de l'application. Vous pouvez utiliser les paramètres généraux de Kaspersky Security for Windows Server pour désigner une période différente (en jours) avant que ces événements ne se produisent. Vous pouvez également configurer les notifications de l'administrateur relatives à ces événements (cf. section "Configuration des notifications de l'administrateur et des utilisateurs" à la page [228](#)).

Kaspersky Security for Windows Server télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky Lab, depuis le Serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.

Vous pouvez télécharger les mises à jour sur chaque serveur protégé ou choisir un serveur en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les ordinateurs. Si vous utilisez Kaspersky Security Center pour l'administration centralisée de la protection des serveurs de l'entreprise, vous pouvez utiliser le Serveur d'administration de Kaspersky Security Center en guise d'intermédiaire pour le téléchargement des mises à jour.

Vous pouvez lancer la tâche de mise à jour des bases de l'application manuellement ou selon une planification (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)). Par défaut, Kaspersky Security for Windows Server lance la tâche Mise à jour des bases de l'application toutes les heures.

Si le téléchargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Security for Windows Server reviendra automatiquement à l'utilisation des dernières mises à jour des bases de données installées. En cas d'endommagement des bases de données de Kaspersky Security for Windows Server, il est possible de revenir manuellement (cf. section "Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server" à la page [190](#)) aux mises à jour antérieures.

## Schémas de mise à jour des bases et des modules 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 de données et des modules logiciels des applications antivirus que vous utilisez dans votre entreprise.

Vous pouvez mettre à jour les bases et les modules de Kaspersky Security for Windows Server 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 les diffuser sur les serveurs au départ de cet ordinateur.



L'intermédiaire peut être n'importe quel ordinateur sur lequel une des applications suivantes est installée :

- Kaspersky Security for Windows Server (un des serveurs protégés) (Schéma 2).
- Serveur d'administration Kaspersky Security Center (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 du réseau.

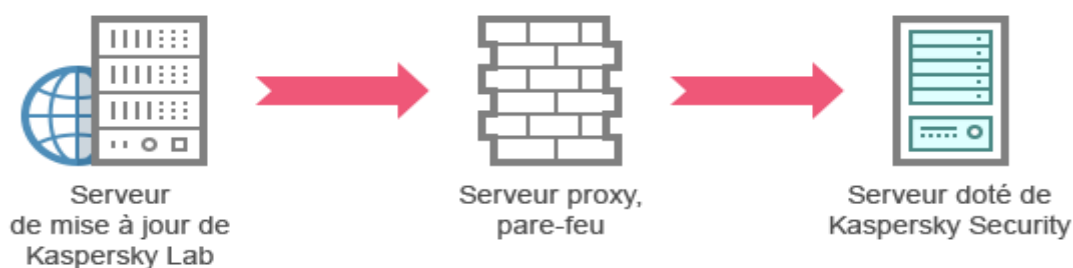
Les différents schémas de mise à jour sont décrits ci-après.

## Schéma 1. Mises à jour des bases de données et des modules directement via Internet

► *Pour configurer les mises à jour de Kaspersky Security for Windows Server directement via Internet :*

dans les paramètres des tâches Mise à jour des bases de l'application et Mise à jour des modules de l'application de chaque serveur protégé, désignez les serveurs de mise à jour de Kaspersky Lab en tant que sources des mises à jour.

En guise de source des mises à jour, vous pouvez indiquer d'autres serveurs HTTP ou FTP qui contiennent un dossier de mise à jour.

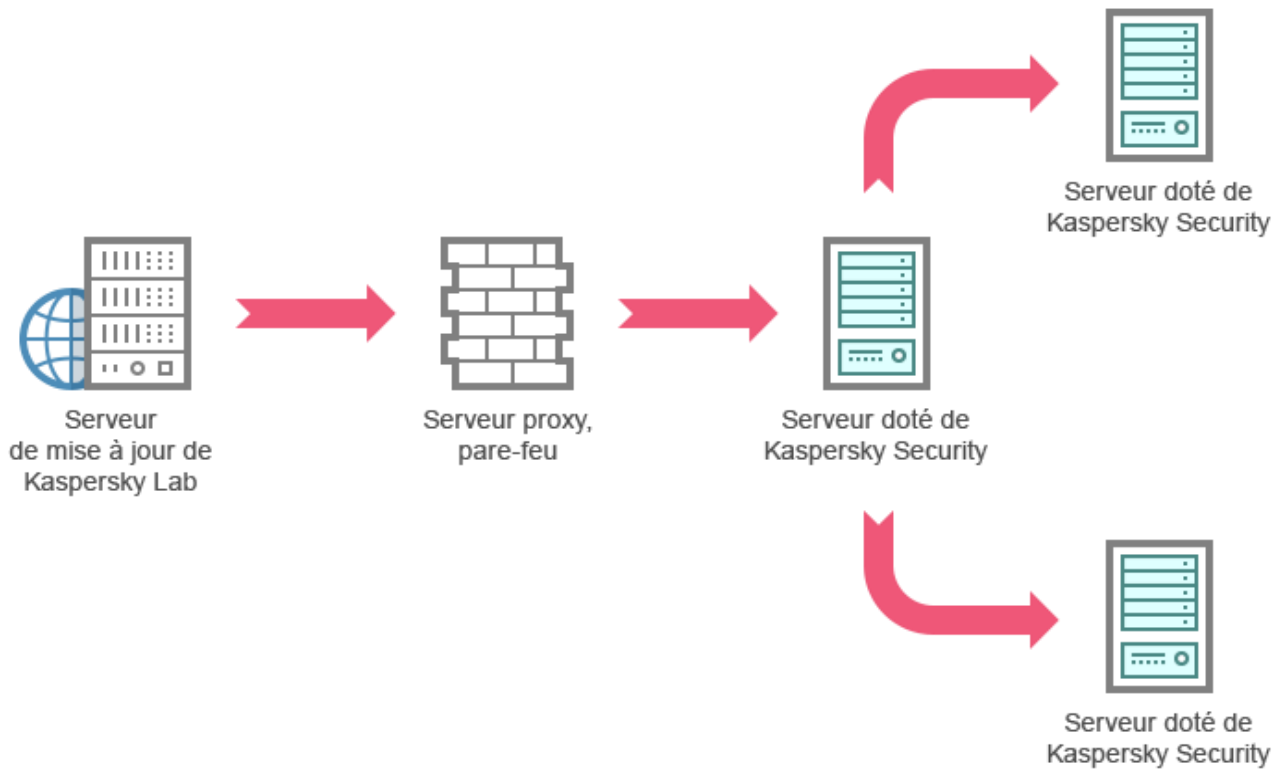


## Schéma 2. Mise à jour des bases de données et des modules via un des serveurs protégés

► *Pour configurer la récupération des mises à jour de Kaspersky Security for Windows Server via un des serveurs protégés, procédez comme suit :*

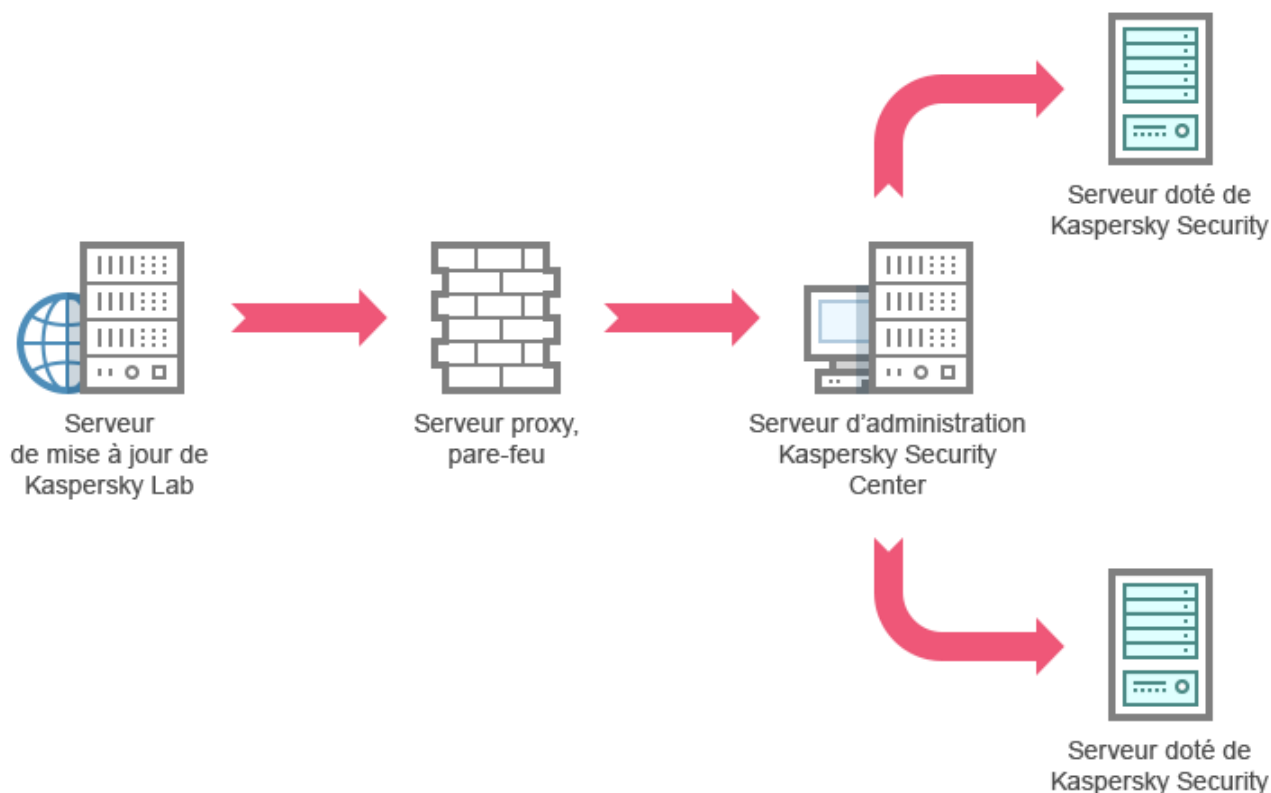
1. Copiez les mises à jour sur le serveur protégé sélectionné. Pour ce faire, procédez comme suit :
  - Sur le serveur sélectionné, configurez les paramètres de la tâche Copie des mises à jour :
    - a. En guise de source des mises à jour, sélectionnez le serveur de mise à jour de Kaspersky Lab.
    - b. Désignez le dossier partagé en guise de dossier d'enregistrement des mises à jour.
2. Diffusez les mises à jour sur les autres serveurs protégés. Pour ce faire, procédez comme suit :
  - Sur chaque serveur protégé, configurez les paramètres de la tâche Mise à jour des bases de l'application (Mise à jour des modules de l'application) (cf. ill. ci-après).
    - a. En guise de source des mises à jour, saisissez le répertoire de l'ordinateur intermédiaire dans lequel vous avez copié les mises à jour.

Kaspersky Security for Windows Server récupérera les mises à jour via un des serveurs protégés.



## Schéma 3. Mise à jour des bases de données et des modules via le Serveur d'administration Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center pour assurer l'administration centralisée de la protection du serveur contre les virus, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Security Center (cf. ill. ci-après).



► Pour configurer la récupération des mises à jour de Kaspersky Security for Windows Server via le Serveur d'administration Kaspersky Security Center, procédez comme suit.

1. Téléchargement des mises à jour depuis le serveur de mise à jour de Kaspersky Lab vers le Serveur d'administration Kaspersky Security Center Pour ce faire, procédez comme suit :
  - Configurez la tâche Réception des mises à jour par le Serveur d'administration pour une sélection d'ordinateurs indiquée :
    - a. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.
2. Diffusez les mises à jour sur les serveurs protégés. Pour ce faire, réalisez une des opérations suivantes :
  - Sur Kaspersky Security Center, configurez une tâche de groupe de mise à jour des bases antivirus (des modules de l'application) afin de diffuser les mises à jour aux serveurs protégés :
    - a. Dans la programmation de la tâche, choisissez la fréquence de démarrage **Après réception des mises à jour par le Serveur d'administration**.

Le Serveur d'administration exécutera la tâche chaque fois qu'il reçoit les mises à jour (cette méthode est la méthode recommandée).

**Vous ne pouvez pas spécifier la fréquence de démarrage **Après réception des mises à jour par le serveur d'administration** dans la console de l'application.**

- Configurez sur chaque serveur protégé les tâches Mise à jour des bases de l'application et Mise à jour des modules de l'application :
  - a. En guise de source des mises à jour, désignez le Serveur d'administration Kaspersky Security Center.
  - b. Le cas échéant, planifiez l'exécution de la tâche.

En cas de mises à jour peu fréquentes des bases antivirus de Kaspersky Security for Windows Server (d'une fois par mois à une fois par an), la probabilité de détecter des menaces diminue tandis que la fréquence des faux positifs augmente dans les composants de l'application.

Kaspersky Security for Windows Server récupérera les mises à jour via le Serveur d'administration Kaspersky Security Center.

Si vous avez l'intention d'utiliser le Serveur d'administration Kaspersky de Security Center pour la diffusion des mises à jour, installez au préalable sur chaque serveur protégé le module logiciel Agent d'administration qui fait partie du kit de distribution de Kaspersky Security Center. Il assure l'interaction entre le Serveur d'administration et Kaspersky Security for Windows Server sur le serveur protégé. Pour obtenir de plus amples informations sur l'Agent d'administration et sa configuration à l'aide de l'application Kaspersky Security Center, consultez l'*aide de Kaspersky Security Center*.

## Configuration des tâches de mise à jour

Cette section contient des instructions sur la configuration des tâches de mise à jour de Kaspersky Security for Windows Server.

### Dans cette section

Configuration des paramètres d'utilisation des sources de mise à jour de Kaspersky Security for Windows Server .....	<a href="#">184</a>
Optimisation de l'utilisation des entrées-sorties du disque lors de l'exécution de la tâche Mise à jour des bases de l'application.....	<a href="#">187</a>
Configuration des paramètres de la tâche Copie des mises à jour.....	<a href="#">188</a>
Configuration des paramètres de la tâche Mise à jour des modules de l'application .....	<a href="#">189</a>

## Configuration des paramètres d'utilisation des sources de mise à jour de Kaspersky Security for Windows Server

Pour chaque tâche de mise à jour, à l'exception de la tâche Annulation de la mise à jour des bases de l'application, il est possible de définir une ou plusieurs sources de mise à jour, d'ajouter des sources de mise à jour définies par l'utilisateur et de configurer les paramètres de connexions aux sources indiquées.

En cas de modification des paramètres des tâches de mises à jour, sachez que les nouvelles valeurs ne sont pas appliquées immédiatement dans les tâches de mise à jour en cours d'exécution. Les nouveaux paramètres seront appliqués uniquement à la prochaine exécution de la tâche.

► Pour déterminer le type de source des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le panneau de détails du nœud sélectionné, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.

4. Dans la section **Source des mises à jour**, sélectionnez le type de source de mises à jour pour Kaspersky Security for Windows Server :

- **Serveur d'administration Kaspersky Security Center**

Kaspersky Security for Windows Server utilise le Serveur d'administration Kaspersky Security Center en tant que source de mise à jour.

Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'accès à distance de Kaspersky Security Center et si l'Agent d'administration (composant de Kaspersky Security Center qui fournit la connexion entre les serveurs et le Serveur d'administration) est installé sur le serveur protégé.

- **Serveurs de mise à jour de Kaspersky Lab**

Kaspersky Security for Windows Server utilise les sites Web de Kaspersky Lab comme source de mises à jour. Ces serveurs hébergent les mises à jour des bases de données et des modules de toutes les applications de Kaspersky Lab.

Cette option est sélectionnée par défaut.

- **Serveurs HTTP, FTP ou dossiers réseau personnalisés**

Kaspersky Security for Windows Server utilise en guise de source de mise à jour le serveur HTTP ou FTP ou les dossiers situés sur le dossier désignés par l'administrateur.

Vous pouvez composer la liste des sources qui contient la sélection la plus récente des mises à jour en cliquant sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

5. Le cas échéant, configurez les paramètres complémentaires des sources de mise à jour définie par l'utilisateur :
  - a. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.
    - i. Dans la fenêtre **Serveurs de mise à jour** qui s'ouvre, cochez ou décochez les cases en regard des sources de mise à jour définies par l'utilisateur afin de commencer à les utiliser ou de suspendre leur utilisation.
    - ii. Cliquez sur le bouton **OK**.
  - b. Dans la section **Source des mises à jour**, sous l'onglet **Général**, cochez ou décochez la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs indiqués ne sont pas disponibles**.

Cette case active ou désactive la fonction d'utilisation des serveurs de mise à jour de Kaspersky Lab en guise de source de mise à jour si les sources que vous avez

sélectionnées ne sont pas disponibles.

Si la case est cochée, la fonction est active.

Cette case est cochée par défaut.

Vous pouvez cocher la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs indiqués ne sont pas disponibles** quand l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** est sélectionnée.

6. Dans la fenêtre **Paramètres de la tâche**, choisissez l'onglet **Paramètres de connexion**, afin de configurer les paramètres de connexion à la source des mises à jour :

- Cochez ou décochez la case **Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky Lab**.

La case active ou désactive l'utilisation des paramètres du serveur proxy si la mise à jour s'opère depuis des serveurs de Kaspersky Lab ou si la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs indiqués ne sont pas disponibles** est cochée.

Si la case est cochée, les paramètres du serveur proxy sont utilisés.

Si la case est décochée, les paramètres du serveur proxy ne sont pas utilisés.

Cette case est cochée par défaut.

- Cochez ou décochez la case **Utiliser les paramètres du serveur proxy pour se connecter aux autres serveurs**.

La case active ou désactive l'utilisation des paramètres du serveur proxy si l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** a été sélectionnée en tant que source des mises à jour.

Si la case est cochée, les paramètres du serveur proxy sont utilisés.

Cette case est décochée par défaut.

Pour des informations sur la configuration des paramètres facultatifs du serveur proxy et d'authentification pour l'accès au serveur proxy, cf. section Lancement et configuration de la tâche de mise à jour des bases de données de Kaspersky Security for Windows Server.

7. Cliquez sur le bouton **OK**.

Les paramètres configurés de la source de mises à jour de Kaspersky Security for Windows Server seront enregistrés et appliqués au prochain lancement de la tâche.

Vous pouvez gérer la liste des sources de mises à jour de Kaspersky Security for Windows Server définies par l'utilisateur.

► *Pour modifier la liste des sources de mises à jour définies par l'utilisateur, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le panneau de détails du nœud sélectionné, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.
4. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

La fenêtre **Serveurs de mise à jour** s'ouvre.

5. Exécutez les actions suivantes :

- Pour ajouter une nouvelle source de mise à jour définie par l'utilisateur, saisissez dans la zone de saisie l'adresse du répertoire contenant les fichiers de mise à jour sur le serveur FTP ou HTTP ; saisissez le répertoire local ou de réseau au format UNC (Universal Naming Convention). Appuyez sur la touche **ENTER**.

Par défaut, le dossier ajouté est utilisé en guise de source de mises à jour.

- Pour suspendre l'utilisation de la source définie par l'utilisateur, décochez la case en regard de la source dans la liste.
- Pour activer l'utilisation de la source définie par l'utilisateur, cochez la case en regard de la source dans la liste.
- Pour modifier l'ordre de sollicitation des sources de mises à jour définies par l'utilisateur pour Kaspersky Security for Windows Server, 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**.
- Pour modifier le chemin d'accès à une source définie par l'utilisateur, sélectionnez la source dans la liste et cliquez sur le bouton **Modifier**. Introduisez les modifications nécessaires dans le champ, puis appuyez sur la touche **RETOUR**.
- Pour supprimer une source définie par l'utilisateur, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

La liste doit toujours compter au moins une source.

6. Cliquez sur le bouton **OK**.

Les modifications introduites dans la liste des sources de mises à jour de l'application définies par l'utilisateur sont enregistrées.

## Optimisation de l'utilisation des entrées-sorties du disque lors de l'exécution de la tâche Mise à jour des bases de l'application

Dans le cadre de l'exécution de la tâche Mise à jour des bases de l'application, Kaspersky Security for Windows Server place les fichiers de la mise à jour sur le disque local du serveur. Vous pouvez réduire la charge sur le sous-système disque du serveur en plaçant les fichiers des mises à jour sur un disque virtuel dans la mémoire vive lors de l'exécution de la mise à jour.

Cette fonction est disponible sous les systèmes d'exploitation Microsoft Windows Vista, Microsoft Windows Server 2008 et les versions plus récentes.

Si vous utilisez cette fonction lors de l'exécution de la tâche Mise à jour des bases de l'application, un disque logique supplémentaire peut apparaître dans le système d'exploitation. Ce disque logique disparaît du système d'exploitation quand la tâche est terminée.



► *Pour réduire la charge sur le sous-système disque de l'ordinateur lors de l'exécution de la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant **Mise à jour des bases de l'application**.
3. Dans le panneau de détails du nœud **Mise à jour des bases de l'application**, cliquez sur le lien **Propriétés**.
4. La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.
5. Configurez les paramètres suivants dans la section Optimisation de l'utilisation des I/O du disque :

- Cochez ou décochez la case **Réduire la charge sur les I/O du disque**.

La case active ou désactive la fonction d'optimisation du sous-système disque grâce à un placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive.

Si la case est cochée, la fonction est active.

Cette case est décochée par défaut.

- Définissez le volume de mémoire vive en méga-octets dans le champ **Volume de mémoire vive utilisé pour l'optimisation**. Le système d'exploitation affecte temporairement ce volume de mémoire vive à l'hébergement des fichiers des mises à jour pendant l'exécution de la tâche. Le volume de mémoire vive défini par défaut est de 512 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

6. Cliquez sur le bouton **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

## Configuration des paramètres de la tâche Copie des mises à jour

► *Pour configurer les paramètres de la tâche Copie des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant **Copie des mises à jour**.
3. Dans le panneau de détails du nœud **Copie des mises à jour**, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Les onglets **Général** et **Paramètres de connexion** permettent de configurer les paramètres d'utilisation des sources de mises à jour (cf. section "Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Security for Windows Server" à la page [184](#)).
5. Dans la section **Paramètres de copie des mises à jour** de l'onglet **Général**, procédez comme suit :

- Définissez les conditions de copie des mises à jour :

- **Copier les mises à jour des bases de l'application.**

Kaspersky Security for Windows Server télécharge uniquement les mises à jour des bases de l'application.

Cette option est sélectionnée par défaut.

- **Copier les mises à jour critiques des modules de l'application.**

Kaspersky Security for Windows Server télécharge uniquement les mises à jour urgentes des modules de l'application Kaspersky Security for Windows Server.

- **Copier les mises à jour des bases de l'application et les mises à jour critiques des modules de l'application.**

Kaspersky Security for Windows Server télécharge les mises à jour des bases de l'application et les mises à jour critiques des modules de Kaspersky Security for Windows Server.

- Indiquez le répertoire local ou de réseau dans lequel Kaspersky Security for Windows Server copiera les mises à jour reçues.
6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)).
  7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page [160](#)).
  8. Cliquez sur le bouton **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

## 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, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant **Mise à jour des modules de l'application**.
3. Dans le panneau de détails du nœud **Mise à jour des modules de l'application**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

4. Les onglets **Général** et **Paramètres de connexion** permettent de configurer les paramètres d'utilisation des sources de mises à jour (cf. section "Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Security for Windows Server" à la page [184](#)).
5. Dans la section **Paramètres de mise à jour de l'application** du groupe **Général**, configurez les paramètres de la mise à jour des modules de l'application :

- **Rechercher uniquement la présence des mises à jour critiques de l'application**

Kaspersky Security for Windows Server signale la présence de mises à jour urgentes des modules de l'application sur la source sans les télécharger. La notification est affichée uniquement si la notification pour ce type d'événement a été configurée.

Cette option est sélectionnée par défaut.

- **Copier et installer les mises à jour critiques des modules de l'application**

Kaspersky Security for Windows Server télécharge et installe les mises à jour critiques des modules de l'application.

- **Autoriser le redémarrage du système d'exploitation**

Redémarrage du système d'exploitation après l'installation de mises à jour qui requièrent le redémarrage.

Si la case est cochée, Kaspersky Security for Windows Server redémarre le système d'exploitation après l'installation des mises à jour qui requièrent le redémarrage.

La case est active si l'option **Copier et installer les mises à jour critiques des modules**

**de l'application** a été sélectionnée.

Cette case est décochée par défaut.

- **Recevoir des informations sur les mises à jour des modules de l'application prévues**

Les notifications sur toutes les mises à jour des modules de Kaspersky Security for Windows Server prévues disponibles sur la source sont affichées. L'application affiche une notification si les notifications de ce type d'événement sont activées.

Si la case est cochée, Kaspersky Security for Windows Server envoie les notifications relatives à toutes les mises à jour prévues des modules de l'application disponibles sur la source de mises à jour.

Cette case est cochée par défaut.

6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)). Par défaut, Kaspersky Security for Windows Server lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).
7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page [160](#)).
8. Cliquez sur le bouton **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement *Une mise à jour prévue des modules de l'application est disponible*. Celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées.

## Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server

Avant d'appliquer la mise à jour des bases de données, Kaspersky Security for Windows Server crée une copie de sauvegarde des bases utilisées antérieurement. Si la mise à jour est interrompue ou se solde par un échec, Kaspersky Security for Windows Server reviendra automatiquement à l'utilisation des mises à jour installées antérieurement.

Si vous rencontrez des problèmes après la mise à jour des bases de données, vous pouvez revenir à l'état antérieur des bases grâce à la tâche Annulation de la mise à jour des bases de l'application.

► *Pour lancer la tâche Annulation de la mise à jour des bases de l'application,*

cliquez sur le lien **Démarrer** dans le panneau de détails du nœud **Annulation de la mise à jour des bases de l'application**.

## Remise à l'état antérieur à la mise à jour des modules de l'application

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Avant d'appliquer la mise à jour des modules de l'application, Kaspersky Security for Windows Server 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 Security for Windows Server reviendra automatiquement à l'utilisation des derniers modules actualisés installés.

Pour revenir à l'état antérieur des modules logiciels, utilisez le composant **Ajout/suppression de programme** du panneau de configuration de Microsoft Windows.

## Statistiques sur les 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, ainsi que d'autres statistiques d'exécution de la tâche.

Vous pouvez consulter ces informations dans le journal d'exécution de la tâche quand la tâche est terminée ou arrêtée.

► *Pour consulter les statistiques de la tâche de mise à jour, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche dont vous souhaitez consulter les statistiques.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Si vous consultez la tâche Mise à jour des bases de l'application ou la tâche Copie des mises à jour, le groupe **Statistiques** affiche le volume de données téléchargées par Kaspersky Security for Windows Server à ce moment (**Données reçues**).

Si vous consultez la tâche Mise à jour des modules de l'application, vous verrez les informations décrites dans le tableau ci-dessous.

Tableau 32. Informations sur la tâche Mise à jour des modules de l'application

Champ	Description
<b>Données reçues</b>	Volume total de données téléchargées
<b>Mises à jour critiques disponibles</b>	Nombre de mises à jour critiques prêtes pour l'installation.
<b>Mises à jour prévues disponibles</b>	Nombre de mises à jour prévues disponibles pour l'installation.

Champ	Description
<b>Erreur d'application des mises à jour</b>	Si la valeur de ce champ est différente de zéro, la mise à jour n'a pas été appliquée. Vous pouvez consulter le nom de la mise à jour pendant laquelle l'erreur s'est produite dans le journal d'exécution de la tâche (cf. section "Consultation des statistiques et informations relatives à la tâche de Kaspersky Security for Windows Server dans les journaux d'exécution des tâches" à la page <a href="#">218</a> ).

## Isolement et copie de sauvegarde des objets

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur l'isolement des fichiers probablement infectés.

### Contenu du chapitre

Isolement des objets probablement infectés.Quarantaine .....	<a href="#">193</a>
Création de copies de sauvegarde des objets.Sauvegarde.....	<a href="#">203</a>
Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués .....	<a href="#">209</a>

## Isolement des objets probablement infectés. Quarantaine

Cette section aborde l'isolement des objets probablement infectés, c.-à-d. le placement de ces objets en quarantaine, et la configuration du stockage de la quarantaine.

### Dans cette section

A propos de l'isolement des objets probablement infectés .....	<a href="#">193</a>
Consultation des objets en quarantaine .....	<a href="#">193</a>
Analyse de la quarantaine .....	<a href="#">195</a>
Restauration du contenu de la quarantaine.....	<a href="#">197</a>
Mise en quarantaine d'objets.....	<a href="#">199</a>
Suppression d'objets de la quarantaine.....	<a href="#">199</a>
Envoi des objets probablement infectés à Kaspersky Lab pour examen.....	<a href="#">200</a>
Configuration des paramètres de la quarantaine .....	<a href="#">201</a>
Statistiques de quarantaine .....	<a href="#">202</a>

## A propos de l'isolement des objets probablement infectés

Kaspersky Security for Windows Server place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers le dossier *Quarantaine*. Pour des raisons de sécurité, une fois dans le dossier Quarantaine, les objets sont chiffrés.

## Consultation des objets en quarantaine

Vous pouvez consulter les objets en quarantaine dans le nœud **Quarantaine** de la console de l'application.

► *Pour consulter les objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.

Les informations relatives aux objets placés en quarantaine apparaissent dans le panneau de détails du nœud sélectionné.

► *Pour trouver l'objet requis dans la liste des objets en quarantaine,*

triez les objets (cf. section "Tri des objets en quarantaine" à la page [194](#)) ou filtrez-les (cf. section Filtrage des objets en quarantaine" à la page [194](#)).

## Dans cette section

Tri des objets en quarantaine .....	<a href="#">194</a>
Filtrage des objets en quarantaine .....	<a href="#">194</a>

## 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 fermez et ouvrez à nouveau le nœud **Quarantaine**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau.

► *Pour trier les objets, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Dans le panneau de résultats du nœud **Quarantaine**, sélectionnez l'en-tête de la colonne selon lequel vous souhaitez trier les objets de la liste.

Les objets de la liste seront triés selon le paramètre sélectionné.

## 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 et ouvrez à nouveau le nœud **Quarantaine**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau à partir de ce fichier.

► *Pour définir un ou plusieurs filtres, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Dans le menu contextuel du nom du nœud, sélectionnez l'option **Filtre**.

La fenêtre **Paramètres du filtre** s'ouvre.



4. Pour ajouter un filtre, procédez comme suit :
  - a. Dans la liste **Nom du champ**, sélectionnez l'élément auquel la valeur du filtre sera comparée.
  - 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 les étapes a à d pour chaque filtre que vous ajoutez. Suivez les recommandations ci-après quand vous utilisez les filtres :

- Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
- Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
- Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
- Pour modifier un filtre, sélectionnez-le dans la liste de la fenêtre **Paramètres du filtre**. Changez ensuite les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer**.

5. Une fois que tous les filtres auront été ajoutés, cliquez sur le bouton **Appliquer**.

Les filtres créés sont enregistrés.

► *Pour afficher à nouveau tous les objets dans la liste des objets en quarantaine,*

sélectionnez l'option **Supprimer** le filtre dans le menu contextuel du nœud **Quarantaine**.

## Analyse de la quarantaine

Par défaut, Kaspersky Security for Windows Server exécute la tâche système Analyse de la quarantaine après chaque mise à jour des bases de l'application. Les paramètres de la tâche sont présentés dans le tableau suivant. Vous ne pouvez pas modifier les paramètres de la tâche Analyse de la quarantaine.

Vous pouvez planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)), la lancer manuellement et modifier les autorisations du compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page [160](#)) sous lequel la tâche est lancée.

Suite à l'analyse des objets en quarantaine après la mise à jour des bases, Kaspersky Security for Windows Server peut décider que certains de ces objets sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés, auquel cas Kaspersky Security for Windows Server exécutera les actions définies dans les paramètres de la tâche Analyse de la quarantaine : désinfecter, supprimer si la désinfection est impossible.

Tableau 33. Paramètres de la tâche Analyse de la quarantaine

Paramètres de la tâche Analyse de la quarantaine	Valeur
Zone d'analyse	Dossier de quarantaine
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; les valeurs possibles sont reprises au tableau suivant.

Tableau 34. Paramètres de sécurité de la tâche Analyse de la quarantaine

Paramètre de sécurité	Valeur
Analyser les objets	Tous les objets de la zone d'analyse
Optimisation	Désactivée
Action à exécuter sur les objets infectés et autres détectés.	Désinfecter, supprimer si la désinfection est impossible
Action à exécuter sur les objets probablement infectés	Rapport uniquement
Exclure les objets	non
Ne pas détecter	non
Arrêter si l'analyse dure plus de (s.)	Non configuré
Ne pas analyser les objets de plus de (Mo)	Non configuré
Analyser les flux NTFS alternatifs	Activée
Secteurs d'amorçage et partition MBR	Désactivée
Utiliser la technologie iChecker	Désactivée
Utiliser la technologie iSwift	Désactivée
Analyser les objets composés	<ul style="list-style-type: none"> <li>• Archives*</li> <li>• Archives SFX*</li> <li>• Objets compactés*</li> <li>• Objets OLE intégrés*</li> </ul> <p>* L'analyse uniquement des nouveaux fichiers et des fichiers modifiés est désactivée.</p>

Paramètre de sécurité	Valeur
Vérification de la signature Microsoft des fichiers	Non exécutée
Utiliser l'analyse heuristique	Appliqué au niveau d'analyse <b>Minutieuse</b>
Zone de confiance	Pas appliqué

## Restauration du contenu de la quarantaine

Kaspersky Security for Windows Server place les objets probablement infectés sous une forme chiffrée dans le dossier 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 **Désinfecté** ;
- Vous estimez que l'objet ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Security for Windows Server n'isole plus cet objet lors des analyses ultérieures, il faut l'exclure du traitement dans la tâche Protection des fichiers en temps réel et des tâches d'analyse à la demande. Pour ce faire, désignez l'objet comme valeur du paramètre de sécurité **Exclure les fichiers** (selon le nom du fichier) ou **Ne pas détecter** dans ces tâches ou ajoutez-le à la Zone de confiance (à la page [520](#)).

Lors de la restauration des objets, vous pouvez sélectionner l'endroit où sera enregistré l'objet : dans l'emplacement d'origine (par défaut), dans un dossier spécial pour objets restaurés sur le serveur protégé ou dans un dossier personnalisé du serveur où est installée la console de l'application, ou sur un autre ordinateur du réseau.

L'option **Restaurer dans le dossier** sert à stocker 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 par les paramètres de la quarantaine.

La restauration d'objets de la quarantaine peut entraîner l'infection du serveur.

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 de données.

Si l'objet placé en quarantaine faisait partie d'un objet composé (une archive par exemple), Kaspersky Security for Windows Server ne l'inclut pas à nouveau dans cet objet lors de la restauration mais l'enregistre séparément dans le dossier indiqué.

Vous pouvez restaurer un ou plusieurs objets.

► *Pour restaurer des objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Dans le panneau de détails du nœud **Quarantaine**, exécutez une des actions suivantes :
  - Pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer ;
  - Pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur un des objets sélectionnés et sélectionnez la commande **Restaurer** dans le menu contextuel.

La fenêtre **Restauration de l'objet** s'ouvre.

4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chacun des objets sélectionnés le dossier dans lequel l'objet à restaurer va être enregistré.

Le nom de l'objet apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous aviez choisi plusieurs objets, le nom du premier objet de la liste des objets sélectionnés s'affiche.

5. Exécutez une des actions suivantes :
  - Pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine** ;
  - Pour restaurer un objet dans le dossier que vous avez défini en tant qu'emplacement de restauration des objets dans les paramètres, sélectionnez **Restaurer dans le dossier par défaut**.
  - Pour restaurer l'objet dans un autre dossier du serveur où vous avez installé la console de l'application for Windows Server ou dans un dossier partagé, sélectionnez **Restaurer dans le dossier de l'ordinateur local ou de la ressource réseau**, puis sélectionnez le dossier souhaité ou saisissez le chemin d'accès à celui-ci.
6. Si vous souhaitez conserver une copie de l'objet dans le dossier de quarantaine après la restauration, décochez la case **Supprimer les objets des stockages après leur restauration**.
7. 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 enregistrés à l'emplacement que vous aurez désigné : si vous avez choisi **Restaurer dans le dossier d'origine**, chacun de ces objets sera enregistré dans son emplacement d'origine ; si vous aviez choisi **Restaurer dans le dossier par défaut** ou **Restaurer dans le dossier de l'ordinateur local ou de la ressource réseau**, tous les objets seront enregistrés dans le dossier indiqué.

8. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server commence par restaurer le premier des objets que vous avez sélectionnés.

9. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.
  - a. Sélectionnez une des actions suivantes de Kaspersky Security for Windows Server :
    - **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, pour appliquer l'action **Remplacer** ou **Renommer**, via l'ajout d'un suffixe au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).
  - c. Cliquez sur le bouton **OK**.

L'objet sera restauré. Les informations relatives à la restauration sont consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, la fenêtre **Restauration de l'objet** s'ouvrira à nouveau. Vous pouvez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 4 des présentes instructions).

## Mise en quarantaine d'objets

Vous pouvez mettre manuellement des fichiers en quarantaine.

► *Pour mettre un fichier en quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Quarantaine**.
2. Choisissez l'option **Ajouter**.
3. Dans la fenêtre **Ouvrir**, sélectionnez le fichier que vous souhaitez placer en quarantaine.
4. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server place le fichier sélectionné en quarantaine.

## Suppression d'objets de la quarantaine

Conformément aux paramètres de la tâche Analyse de la quarantaine, Kaspersky Security for Windows Server 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 si Kaspersky Security for Windows Server n'avait pas réussi à les désinfecter. Kaspersky Security for Windows Server ne supprime pas les autres objets de la Quarantaine.

Vous pouvez supprimer manuellement un ou plusieurs objets de la quarantaine.

► *Pour supprimer un ou plusieurs objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Exécutez une des actions suivantes :
  - Pour supprimer un objet, choisissez l'option **Supprimer** dans le menu contextuel du nom de l'objet.
  - Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez l'option **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

Les objets sélectionnés seront supprimés de la quarantaine.

## Envoi des objets probablement infectés à Kaspersky Lab pour examen

Si le comportement d'un fichier indique selon vous la présence éventuelle d'une menace et que Kaspersky Security for Windows Server le considère comme un fichier sain, il se peut que vous soyez en présence d'une menace inconnue dont la signature n'a pas encore été ajoutée aux bases de données. 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 Security for Windows Server le considère comme un fichier infecté et parvienne à le désinfecter. 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. Les fichiers en quarantaine sont conservés sous forme cryptée et lors de transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

**Vous ne pouvez pas envoyer un objet de la quarantaine à Kaspersky Lab une fois que la licence n'est plus valide.**

► *Pour envoyer un fichier à Kaspersky Lab pour examen, procédez comme suit :*

1. Si le fichier ne se trouve pas déjà en quarantaine, placez-le à titre préventif en **Quarantaine**.
2. Dans le nœud **Quarantaine**, dans la liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous souhaitez envoyer à Kaspersky Lab pour examen et sélectionnez l'option **Envoyer l'objet pour analyse**.
3. Dans la fenêtre de confirmation de l'opération, cliquez sur **Oui** si vous voulez vraiment envoyer l'objet sélectionné pour le soumettre à un examen.
4. Si un client de messagerie est configuré sur le serveur où la console de l'application est installée, un nouveau message électronique est créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

Le champ **Destinataire** du message contient l'adresse email de Kaspersky Lab [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com). Le champ **Objet** contient le texte "Objet de la quarantaine".

Le corps du message contiendra le texte suivant : "Ce fichier va être envoyé à Kaspersky Lab pour analyse". Vous pouvez reprendre dans le corps du message n'importe quelle information complémentaire sur le fichier : raisons pour lesquelles il vous semble probablement infecté ou dangereux, son comportement et ses effets sur le système.

Le message est accompagné de l'archive <nom de l'objet>.cab. L'archive contient le fichier <uuid>.klq avec l'objet chiffré, le fichier <uuid>.txt avec les informations extraites par Kaspersky Security for Windows Server sur l'objet et le fichier Sysinfo.txt qui contient les informations relatives à Kaspersky Security for Windows Server et au système d'exploitation du serveur :

- Nom et version du système d'exploitation.
- Nom et version de Kaspersky Security for Windows Server.
- Date de publication des dernières mises à jour des bases de l'application installées.
- Clé active.

Ces informations sont indispensables aux experts en antivirus 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.

Si aucun client de messagerie n'est installé sur le serveur où se trouve la console de l'application, l'application vous demande d'enregistrer l'objet chiffré sélectionné dans un fichier. Ce fichier peut être envoyé seul à Kaspersky Lab.

► *Pour enregistrer l'objet crypté dans un fichier, procédez comme suit :*

1. Dans la fenêtre qui vous invite à enregistrer l'objet, cliquez sur le bouton **OK**.
2. Sélectionnez le répertoire sur le disque du serveur protégé ou le répertoire de réseau dans lequel vous souhaitez enregistrer le fichier avec l'objet.

L'objet sera enregistré dans un fichier au format CAB.

## Configuration des paramètres de la quarantaine

Vous pouvez configurer les paramètres de la quarantaine. Les nouveaux paramètres de la quarantaine sont appliqués immédiatement après l'enregistrement.

► *Pour configurer les paramètres de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Quarantaine**.
3. Choisissez l'option **Propriétés**.
4. Dans la fenêtre **Propriétés de la quarantaine**, configurez les paramètres requis de la quarantaine en fonction de vos besoins :

- Dans la section **Paramètres de quarantaine** :

- **Dossier de quarantaine**

Chemin d'accès au dossier de la quarantaine au format UNC (Universal Naming Convention).

Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\.

- **Taille maximale de la quarantaine**

La case active ou désactive la fonction qui surveille le volume total des objets placés en quarantaine. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Security for Windows Server consigne l'événement *Dépassement de la taille maximum de la quarantaine* et publie une notification conformément aux paramètres pour ce type d'événements.

Si la case est cochée, Kaspersky Security for Windows Server surveille le volume total des objets placés en quarantaine.

Si la case est décochée, Kaspersky Security for Windows Server ne surveille pas le volume total des objets placés en quarantaine.

Cette case est décochée par défaut.

- **Seuil d'espace disponible**

La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil,



Kaspersky Security for Windows Server consigne l'événement *Dépassement du seuil d'espace libre disponible dans la sauvegarde* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

Si la case est cochée, Kaspersky Security for Windows Server surveille le volume d'espace disponible dans la sauvegarde.

La case *Seuil d'espace disponible (Mo)* est active si la case *Taille maximale de sauvegarde (Mo)* a été cochée.

Cette case est cochée par défaut.

Si le volume des objets en quarantaine dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Security for Windows Server vous le signale sans arrêter de placer les objets en quarantaine.

- Dans la section **Paramètres de restauration** :
  - **Dossier cible pour la restauration des objets**

5. Cliquez sur le bouton **OK**.

Les paramètres de la quarantaine définis seront enregistrés.

## 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,*

choisissez l'option **Statistiques** dans le menu contextuel du nœud **Quarantaine** de l'arborescence de la console de l'application.

La fenêtre **Statistiques** reprend les informations sur le nombre d'objets en quarantaine à l'heure actuelle (cf. tableau ci-dessous).

Champ	Description
<b>Objets probablement infectés</b>	Nombre d'objets découverts par Kaspersky Security for Windows Server et considérés comme probablement infectés.
<b>Espace de quarantaine utilisé</b>	Volume général de données dans le dossier de quarantaine.
<b>Fausses alertes</b>	Nombre d'objets qui ont reçu l'état <i>Fausse alerte</i> car l'analyse de la quarantaine à l'aide des bases mises à jour a indiqué que ces objets étaient non infectés.
<b>Objets désinfectés</b>	Nombre d'objets qui ont reçu l'état <i>Désinfectés</i> après l'analyse de la quarantaine.
<b>Nombre total d'objets</b>	Nombre total d'objets en quarantaine.

## Création de copies de sauvegarde des objets. Sauvegarde

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur la configuration des paramètres de la Sauvegarde.

### Dans cette section

A propos de la Sauvegarde des objets avant la désinfection ou la suppression .....	<a href="#">203</a>
Consultation des objets dans la sauvegarde .....	<a href="#">203</a>
Restauration des fichiers depuis la sauvegarde .....	<a href="#">205</a>
Suppression des fichiers de la Sauvegarde .....	<a href="#">207</a>
Configuration des paramètres de la Sauvegarde .....	<a href="#">207</a>
Statistiques de sauvegarde .....	<a href="#">208</a>

### A propos de la Sauvegarde des objets avant la désinfection ou la suppression

Kaspersky Security for Windows Server enregistre une copie chiffrée des objets dont le statut est *Infecté* ou *Probablement infecté* dans la *Sauvegarde* avant de procéder à la désinfection ou à la suppression de ces objets.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Security for Windows Server enregistre cet objet composé complet dans la sauvegarde. Par exemple, si Kaspersky Security for Windows Server considère un des objets de la base de messagerie comme étant infecté, il place l'ensemble de la base de messagerie dans la sauvegarde.

Si la taille de l'objet que Kaspersky Security for Windows Server copie dans la sauvegarde est importante, le système peut ralentir et l'espace disponible sur le disque dur peut diminuer.

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 depuis la sauvegarde si, par exemple, le fichier original infecté contenait des informations cruciales et que lors de la désinfection, Kaspersky Security for Windows Server n'a pas réussi à le préserver, ce qui a rendu inaccessibles les informations qu'il contenait.

La restauration de fichiers de la Sauvegarde peut provoquer l'infection de l'ordinateur.

### Consultation des objets dans la sauvegarde

Vous pouvez consulter les objets du dossier de sauvegarde uniquement via la console de l'application sous le nœud **Sauvegarde**. Vous ne pouvez pas les consulter à l'aide des gestionnaires de fichiers de Microsoft Windows.

► *Pour consulter les objets de la Sauvegarde,*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.

- Sélectionnez le nœud enfant **Sauvegarde**.

Les informations relatives aux objets placés dans la sauvegarde apparaissent dans le panneau de détails du nœud sélectionné.

- *Pour trouver l'objet requis dans la liste des objets de la Sauvegarde, triez les objets ou filtrez-les.*

## Dans cette section

Tri des fichiers de la Sauvegarde .....	<a href="#">204</a>
Filtrage des fichiers de la Sauvegarde .....	<a href="#">204</a>

## 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 de résultats.

Les résultats du tri sont préservés si vous quittez le nœud **Sauvegarde** et que vous l'ouvrez à nouveau ou si vous fermez la console de l'application, enregistrez le fichier msc et que vous l'ouvrez à nouveau depuis ce fichier.

- *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

- Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
- Sélectionnez le nœud enfant **Sauvegarde**.
- Dans la liste des fichiers de la **Sauvegarde**, sélectionnez l'en-tête de la colonne selon laquelle vous souhaitez trier les objets.

Les fichiers de la Sauvegarde seront triés en fonction du critère sélectionné.

## 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 nœud **Sauvegarde** uniquement les fichiers qui répondent aux conditions de filtrage que vous avez définies (les filtres).

Les résultats du tri sont enregistrés si vous quittez le nœud **Sauvegarde** et que vous l'ouvrez à nouveau, ou si vous fermez la console de l'application, enregistrez le fichier msc et que vous l'ouvrez à nouveau depuis ce fichier.

- *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

- Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Sauvegarde** et choisissez l'option **Filtre**.  
La fenêtre **Paramètres du filtre** s'ouvre.
- Pour ajouter un filtre, procédez comme suit :
  - Dans la liste **Nom du champ**, sélectionnez le champ dont la valeur sera comparée à la valeur du filtre.
  - 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.
- 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 chacun des filtres ajoutés. Les consignes suivantes peuvent intervenir dans l'utilisation des filtres :

- Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
- Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
- 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 fenêtre **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer**.

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 tous les fichiers dans la liste des fichiers dans la sauvegarde,*

sélectionnez l'option **Supprimer le filtre** dans le menu contextuel du nœud **Sauvegarde**.

## Restauration des fichiers depuis la Sauvegarde

Kaspersky Security for Windows Server place les fichiers dans la sauvegarde sous forme chiffrée 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 Security for Windows Server n'a pas pu préserver son intégrité et que les informations qu'il contenait sont devenues par conséquent inaccessibles.
- Vous estimez que le fichier ne présente aucun danger pour le serveur et vous souhaitez l'utiliser. Afin que Kaspersky Security for Windows Server ne considère plus ce fichier comme un fichier infecté ou probablement infecté lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche Protection des fichiers en temps réel et dans les tâches d'analyse à la demande. Pour ce faire désignez le fichier en tant que valeur du paramètre **Exclure les fichiers** ou du paramètre **Ne pas détecter** dans les tâches correspondantes.

La restauration de fichiers de la Sauvegarde peut provoquer l'infection de l'ordinateur.

Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où il sera enregistré : dans l'emplacement d'origine (par défaut), dans un dossier spécial pour objets restaurés sur le serveur protégé ou dans un dossier personnalisé sur le serveur où la console de l'application 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 au dossier est défini dans les paramètres de la Sauvegarde (cf. section "Configuration des paramètres de la Sauvegarde" à la page [207](#)).

Par défaut, quand Kaspersky Security for Windows Server restaure un fichier, il enregistre une copie dans la sauvegarde. Vous pouvez supprimer la copie du fichier de la Sauvegarde après la restauration.

► *Pour restaurer des fichiers depuis la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Sauvegarde**.
3. Dans le panneau de détails du nœud **Sauvegarde**, exécutez une des actions suivantes :
  - Pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer ;
  - Pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur un des objets sélectionnés et sélectionnez la commande **Restaurer** dans le menu contextuel.

La fenêtre **Restauration de l'objet** s'ouvre.

4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chacun des objets sélectionnés le dossier dans lequel l'objet à restaurer va être enregistré.

Le nom de l'objet apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous avez choisi plusieurs objets, le nom du premier objet de la liste des objets sélectionnés s'affiche.

5. Exécutez une des actions suivantes :
  - Pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine** ;
  - Pour restaurer un objet dans le dossier que vous avez défini en tant qu'emplacement de restauration des objets dans les paramètres, sélectionnez **Restaurer dans le dossier par défaut**.
  - Pour restaurer l'objet dans un autre dossier du serveur où vous avez installé la console de l'application for Windows Server ou dans un dossier partagé, sélectionnez **Restaurer dans le dossier de l'ordinateur local ou de la ressource réseau**, puis sélectionnez le dossier souhaité ou saisissez le chemin d'accès à celui-ci.
6. Si vous ne souhaitez pas conserver une copie du fichier dans la sauvegarde après la restauration, cochez la case **Supprimer les objets des stockages après leur restauration** (case décochée par défaut)
7. 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 enregistrés à l'emplacement que vous aurez désigné : si vous avez choisi **Restaurer dans le dossier d'origine**, chacun de ces objets sera enregistré dans son emplacement d'origine ; si vous aviez choisi **Restaurer dans le dossier par défaut** ou **Restaurer dans le dossier de l'ordinateur local ou de la ressource réseau**, tous les objets seront enregistrés dans le dossier indiqué.

8. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server commence par restaurer le premier des objets que vous avez sélectionnés.

9. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.
  - a. Sélectionnez une des actions suivantes de Kaspersky Security for Windows Server :
    - **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, pour appliquer l'action **Remplacer** ou **Renommer**, via l'ajout d'un suffixe au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).
  - c. Cliquez sur le bouton **OK**.

L'objet sera restauré. Les informations relatives à la restauration sont consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, la fenêtre **Restauration de l'objet** s'ouvrira à nouveau. Vous pouvez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 4 des présentes instructions).

## Suppression des fichiers de la Sauvegarde

► *Pour supprimer un ou plusieurs fichiers de la Sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Sauvegarde**.
3. Exécutez une des actions suivantes :
  - Pour supprimer un objet, choisissez l'option **Supprimer** dans le menu contextuel du nom de l'objet.
  - Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez l'option **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

Les fichiers sélectionnés seront supprimés de la Sauvegarde.

## Configuration des paramètres de la Sauvegarde

► *Pour configurer les paramètres de la Sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Sauvegarde**.
3. Choisissez l'option **Propriétés**.
4. Dans la fenêtre **Propriétés de la Sauvegarde**, configurez les paramètres requis de la Sauvegarde en fonction de vos besoins :

Dans la section **Paramètres de la Sauvegarde** :

- **Dossier de sauvegarde**

Chemin d'accès à la sauvegarde au format UNC (Universal Naming Convention).

Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\.

- **Taille maximale de sauvegarde (Mo)**

La case active ou désactive la fonction qui surveille le volume total des objets placés dans la Sauvegarde. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Security for Windows Server consigne l'événement *Dépassement de la taille maximale de la Sauvegarde* et publie une notification conformément aux paramètres pour ce type d'événements.

Si la case est cochée, Kaspersky Security for Windows Server surveille le volume total des objets placés dans la Sauvegarde.

Si la case est décochée, Kaspersky Security for Windows Server ne surveille pas le volume total des objets placés dans la Sauvegarde.

Cette case est décochée par défaut.

- **Seuil d'espace disponible (Mo)**

La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil, Kaspersky Security for Windows Server consigne l'événement *Dépassement du seuil d'espace libre disponible dans la sauvegarde* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

Si la case est cochée, Kaspersky Security for Windows Server surveille le volume d'espace disponible dans la sauvegarde.

La case Seuil d'espace disponible (Mo) est active si la case Taille maximale de sauvegarde (Mo) a été cochée.

Cette case est cochée par défaut.

Si le volume des objets de la Sauvegarde dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Security for Windows Server vous le signale sans arrêter de placer les objets dans la Sauvegarde.

Dans la section **Paramètres de restauration** :

- **Dossier cible pour la restauration des objets**

Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

Chemin par défaut : C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Restored\.

5. Cliquez sur le bouton **OK**.

Les paramètres configurés de la Sauvegarde seront enregistrés.

## Statistiques de sauvegarde

Vous pouvez consulter les informations relatives à l'état de la Sauvegarde en ce moment : statistiques de



sauvegarde.

► *Pour consulter les statistiques de la Sauvegarde,*

dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez **Statistiques**. La fenêtre **Statistiques de sauvegarde** s'ouvre.

La fenêtre **Statistiques de sauvegarde** reprend les informations relatives à l'état de la Sauvegarde à l'heure actuelle (cf. tableau ci-dessous).

Tableau 35. Informations sur l'état de la Sauvegarde

Champ	Description
<b>Taille actuelle de la Sauvegarde</b>	Volume de données dans la sauvegarde ; tient compte de la taille des fichiers chiffrés
<b>Nombre total d'objets</b>	Nombre d'objets présents actuellement dans la sauvegarde

## Interdire l'accès aux ressources réseau. Liste des ordinateurs bloqués

Cette section décrit comment bloquer les ordinateurs bloqués et configurer les paramètres du Stockage des ordinateurs bloqués.

### Dans cette section

A propos du stockage des ordinateurs bloqués .....	<a href="#">209</a>
Activation du blocage des hôtes douteux .....	<a href="#">210</a>
Configuration des paramètres de la Liste des ordinateurs bloqués .....	<a href="#">211</a>

### A propos du stockage des ordinateurs bloqués

Le Stockage des ordinateurs bloqués est installé par défaut si un des composants suivants est installé : Protection des fichiers en temps réel, Protection contre le chiffrement pour NetApp, Protection contre le chiffrement. Ces composants détectent les tentatives de chiffrement, d'ouverture ou d'exécution d'objets sur les dossiers réseau partagés du serveur protégé ou du périphérique de stockage NAS conformément à la liste des ordinateurs bloqués. Les informations relatives aux hôtes bloqués de tous les serveurs protégés sont envoyées au Kaspersky Security Center. Kaspersky Security for Windows Server bloque l'accès aux dossiers partagés ou aux dossiers de périphériques de stockage NAS pour tous les ordinateurs distants dans la liste des ordinateurs bloqués.

Le Stockage des ordinateurs bloqués est rempli quand au moins une des tâches suivantes est lancée en mode actif et quand les conditions indiquées sont remplies :

- Pour la tâche Protection des fichiers en temps réel : détection d'une activité malveillante émanant d'un ordinateur qui accède aux ressources de fichier réseau ; dans les paramètres de la tâche Protection des fichiers en temps réel, la case **Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante** est cochée.
- Pour la tâche Protection contre le chiffrement : détection d'un chiffrement malveillant réalisé par un

ordinateur qui accède aux ressources de fichier réseau.

- Pour la tâche Protection contre le chiffrement pour NetApp : détection d'une attaque contre le périphérique de stockage NAS.

Après la détection d'une activité ou d'une tentative de chiffrement malveillant, la tâche envoie les informations relatives à l'hôte à l'origine de l'attaque au stockage des ordinateurs bloqués et l'application génère un avertissement de blocage de l'hôte. Toutes les tentatives d'accès aux dossiers réseau partagés réalisées au départ de cet hôte seront bloquées.

Si l'identifiant unique local (LUID) d'un hôte à l'origine de l'attaque a été ajoutée à la liste des ordinateurs bloqués, Kaspersky Security for Windows Server détermine l'adresse IP de cet hôte et ajoute cette adresse IP à la liste des ordinateurs bloqués au lieu de l'identifiant unique local (LUID) d'un hôte à l'origine de l'attaque.

Par défaut, Kaspersky Security for Windows Server supprime les ordinateurs bloqués de la liste 30 minutes après leur ajout. L'accès de l'ordinateur aux ressources de fichier réseau est rétabli automatiquement après sa suppression de la liste des ordinateurs bloqués. Vous pouvez indiquer la durée au terme de laquelle les ordinateurs bloqués sont automatiquement débloqués.

Remarque : lorsque vous limitez l'accès pour la gestion des stockages pour n'importe quel compte utilisateur, le stockage des ordinateurs bloqués reste disponible. Les paramètres Liste des ordinateurs bloqués ne sont pas modifiables, uniquement si le compte utilisateur ne bénéficie pas des droits **Modifier les privilèges** pour l'administration de Kaspersky Security for Windows Server.

## Activation du blocage des hôtes douteux

Pour ajouter des hôtes qui affichent une activité malveillante ou de chiffrement malveillant quelconque à la **liste des ordinateurs bloqués** et bloquer l'accès aux ressources de fichier réseau pour ces hôtes, au moins une des tâches suivantes doit être exécutée en mode actif :

- Protection des fichiers en temps réel
- Protection contre le chiffrement
- Protection contre le chiffrement pour NetApp

### ► Configuration de la tâche Protection des fichiers en temps réel :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

4. Dans la section **Intégration aux autres composants**, cochez la case **Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante** si vous souhaitez que Kaspersky Security for Windows Server bloque les hôtes sur lesquels une activité malveillante a été détectée pendant l'exécution de la tâche Protection des fichiers en temps réel.
5. Si la tâche n'a pas été lancée, ouvrez l'onglet **Planification** :
  - a. Cochez la case **Exécuté selon la programmation**.

- b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

► *Configurez la tâche Protection contre le chiffrement :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général**, assurez-vous que la tâche est en mode **Actif**.
5. Si la tâche n'a pas été lancée, ouvrez l'onglet **Planification** :
  - a. Cochez la case **Exécuté selon la programmation**.
  - b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.  
Les paramètres de la tâche définis seront enregistrés.

► *Configurez la tâche Protection contre le chiffrement pour NetApp :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection des stockages réseau**.
2. Sélectionnez le sous-nœud **Protection contre le chiffrement pour NetApp**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général**, assurez-vous que la tâche est en mode **Actif**.
5. Si la tâche n'a pas été lancée, ouvrez l'onglet **Planification** :
  - a. Cochez la case **Exécuté selon la programmation**.
  - b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

Kaspersky Security for Windows Server bloque l'accès aux ressources de fichier réseau pour les hôtes qui affichent une activité malveillante ou de chiffrement.

## Configuration des paramètres de la Liste des ordinateurs bloqués

► *Pour configurer le stockage des ordinateurs bloqués.*

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Liste des ordinateurs bloqués**.
3. Sélectionnez l'option de menu **Propriétés**.  
La fenêtre **Paramètres de stockage des ordinateurs bloqués** s'affiche.
4. Dans la section **Paramètres du blocage des hôtes**, indiquez le nombre de jours, d'heures et de minutes à

décompter à partir du moment du blocage des hôtes et au terme desquels les hôtes bloqués sont de nouveau autorisés à accéder aux ressources de fichier réseau.

5. Cliquez sur le bouton **OK**.
6. Pour restaurer l'accès à toute la liste des ordinateurs bloqués, procédez comme suit :
  - a. Ouvrez le menu contextuel du nœud enfant **Liste des ordinateurs bloqués**.
  - b. Sélectionnez l'option **Débloquer tout**.

Tous les hôtes seront retirés de la liste et débloqués.
7. Pour retirer plusieurs hôtes de la liste des ordinateurs bloqués, procédez comme suit :
  - a. Dans la liste des ordinateurs bloqués affichée dans le panneau de détails, sélectionnez un ou plusieurs hôtes.
  - b. Ouvrez le menu contextuel du nœud enfant **Liste des ordinateurs bloqués**.
  - c. Sélectionnez l'option **Débloquer la sélection**.

Les hôtes sélectionnés sont débloqués.

## Enregistrement des événements. Journaux de Kaspersky Security for Windows Server

Cette section contient des informations sur l'utilisation des journaux de Kaspersky Security for Windows Server : journal d'audit système, journaux d'exécution des tâches et journal des événements.

### Contenu du chapitre

Méthodes d'enregistrement des événements de Kaspersky Security for Windows Server .....	<a href="#">213</a>
Journal d'audit système .....	<a href="#">214</a>
Journaux d'exécution de la tâche .....	<a href="#">216</a>
Journaux de sécurité .....	<a href="#">220</a>
Consultation du journal des événements de Kaspersky Security for Windows Server dans l'observateur d'événements.....	<a href="#">220</a>
Configuration des paramètres des journaux dans la console de Kaspersky Security for Windows Server .....	<a href="#">221</a>

## Méthodes d'enregistrement des événements de Kaspersky Security for Windows Server

Les événements de Kaspersky Security for Windows Server sont scindés en deux groupes :

- événements liés au traitement des objets dans les tâches de Kaspersky Security for Windows Server ;
- événements liés à l'administration de Kaspersky Security for Windows Server, par exemple lancement d'une application, création ou suppression de tâches, exécution de tâches, modification des paramètres d'une tâche.

Kaspersky Security for Windows Server enregistre les événements dans le journal à l'aide des méthodes suivantes :

- **Journaux d'exécution de la tâche.** Le journal d'exécution de la tâche contient des informations sur l'état actuel de paramètres de la tâche ou sur les événements survenus pendant l'exécution de la tâche.
- **Journal d'audit système.** Le journal d'audit système contient les informations relatives aux événements en rapport avec l'administration de Kaspersky Security for Windows Server.
- **Journal des événements.** Le journal des événements contient les informations relatives aux événements nécessaires au diagnostic des échecs de fonctionnement de Kaspersky Security for Windows Server. Ce journal est accessible dans la console Observateur d'événements de Microsoft Windows.
- **Journaux de sécurité.** Les Journaux de sécurité contiennent les informations relatives aux événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le serveur protégé.

Si un problème survient durant l'utilisation de Kaspersky Security for Windows Server (par exemple, Kaspersky Security for Windows Server ou une tâche particulière s'arrête suite à une erreur ou ne démarre pas) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un fichier de trace et un fichier dump de la mémoire des processus de Kaspersky Security for Windows Server et envoyer ces fichiers avec ces informations au Support Technique de Kaspersky Lab afin de diagnostiquer le problème rencontré.

Kaspersky Security for Windows Server n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par l'utilisateur avec les droits correspondants.

Kaspersky Security for Windows Server consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Security for Windows Server. Vous pouvez configurer les autorisations d'accès (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)) et autoriser l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs requis.

## Journal d'audit système

Kaspersky Security for Windows Server réalise un audit système des événements liés à l'administration de Kaspersky Security for Windows Server. L'application enregistre les informations relatives, par exemple, au lancement de l'application, au lancement et à l'arrêt de tâches de Kaspersky Security for Windows Server, aux modifications des paramètres des tâches, à la création et à la suppression de tâches d'analyse à la demande. Les enregistrements de l'ensemble de ces événements apparaissent dans le panneau de détails lorsque vous sélectionnez le nœud **Journal d'audit système** dans la console de l'application.

Par défaut, Kaspersky Security for Windows Server conserve les entrées du journal d'audit système pendant une durée illimitée. Vous pouvez spécifier la période de stockage des enregistrements dans le journal d'audit système.

Vous pouvez désigner un dossier dans lequel Kaspersky Security for Windows Server va stocker les fichiers du journal d'audit système, différent du dossier choisi par défaut.

### Dans cette section

Tri des événements dans le journal d'audit système.....	<a href="#">214</a>
Consultation de la liste des événements dans les journaux d'exécution des tâches.....	<a href="#">215</a>
Filtrage des événements dans le journal d'audit système.....	<a href="#">215</a>
Suppression d'événements du journal d'audit système.....	<a href="#">216</a>

### Tri des événements dans le journal d'audit système

Par défaut, les événements sont classés dans le nœud du journal d'audit système par ordre chronologique inverse.

Vous pouvez les trier selon le contenu de n'importe quelle colonne, à l'exception de la colonne **Événement**.

► *Pour trier les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez le nœud enfant **Journal d'audit système**.

3. Dans le panneau de détails, sélectionnez l'en-tête de la colonne que vous souhaitez utiliser pour trier les événements de la liste.

Les résultats triés sont enregistrés jusqu'à la prochaine session d'affichage du journal d'audit système.

## Consultation de la liste des événements dans les journaux d'exécution des tâches

► *Pour consulter la liste des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.

La liste des événements consignés dans les journaux d'exécution des tâches de Kaspersky Security for Windows Server apparaît dans le panneau de détails.

Vous pouvez les trier selon le contenu de n'importe quelle colonne ou appliquer un filtre.

## Filtrage des événements dans le journal d'audit système

Vous pouvez configurer le journal d'audit système pour afficher uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage (filtres) que vous définissez.

► *Pour filtrer les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez l'option **Filtre**.

La fenêtre **Paramètres du filtre** s'ouvre.

3. Pour ajouter un filtre, procédez comme suit :
  - a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez filtrer les événements.
  - b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.
  - c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.
  - d. Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.

4. Le cas échéant, réalisez une des opérations suivantes :
  - Afin de réunir quelques filtres à l'aide de l'opérateur logique "ET", sélectionnez l'option **Quand toutes les conditions sont remplies**.
  - Afin de réunir quelques filtres à l'aide de l'opérateur logique "OU", sélectionnez l'option **Quand n'importe quelle condition est remplie**.
5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements du journal d'audit système.

La liste des événements du journal d'audit système affiche uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est enregistré jusqu'à prochaine session d'affichage du journal d'audit système.



► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez **Supprimer le filtre**.  
La liste des événements du journal d'audit système affiche alors tous les événements.

## Suppression d'événements du journal d'audit système

Par défaut, Kaspersky Security for Windows Server conserve les entrées du journal d'audit système pendant une durée illimitée. Vous pouvez spécifier la période de stockage des enregistrements dans le journal d'audit système.

Vous pouvez supprimer manuellement tous les événements du journal d'audit système.

► *Pour supprimer des événements du journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez **Effacer**.
3. Exécutez une des actions suivantes :
  - Si vous souhaitez exporter le contenu du journal d'audit système dans un fichier au format CSV ou TXT avant de supprimer les événements, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de la suppression. Indiquez le nom et l'emplacement du fichier dans la fenêtre qui s'ouvre.
  - Si vous ne souhaitez pas exporter le contenu du journal dans un fichier, cliquez sur le bouton **Non** dans la fenêtre de confirmation de la suppression.

Le contenu du journal d'audit système est effacé.

## Journaux d'exécution de la tâche

Cette section contient des informations relatives aux journaux d'exécution des tâches de Kaspersky Security for Windows Server et des instructions sur leur administration.

### Dans cette section

A propos des journaux d'exécution des tâches .....	<a href="#">216</a>
Tri des événements dans les journaux d'exécution des tâches .....	<a href="#">217</a>
Filtrage des événements dans les journaux d'exécution des tâches .....	<a href="#">217</a>
Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security for Windows Server dans les journaux d'exécution des tâches .....	<a href="#">218</a>
Exportation des informations depuis le journal d'exécution de la tâche .....	<a href="#">219</a>
Suppression des événements des journaux d'exécution des tâches .....	<a href="#">219</a>

### A propos des journaux d'exécution des tâches

Les informations relatives à l'exécution des tâches de Kaspersky Security for Windows Server apparaissent dans le

panneau de détails quand vous sélectionnez le nœud **Journaux d'exécution de la tâche** dans la console de l'application.

Le journal d'exécution de chaque tâche permet de voir les statistiques de l'exécution de la tâche, les informations relatives à chaque objet traité par l'application depuis le lancement de la tâche jusqu'à maintenant ainsi que les paramètres de la tâche.

Par défaut, Kaspersky Security for Windows Server conserve les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez désigner un dossier différent du dossier par défaut dans lequel Kaspersky Security for Windows Server va enregistrer les fichiers des journaux d'exécution des tâches. Vous pouvez également sélectionner les événements qui seront consignés dans les journaux d'exécution des tâches de Kaspersky Security for Windows Server.

## Tri des événements dans les journaux d'exécution des tâches

Par défaut, les événements sont classés dans les journaux d'exécution des tâches par ordre chronologique inverse. Vous pouvez les trier selon le contenu de n'importe quelle colonne.

► *Pour trier les événements repris dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le panneau de détails, sélectionnez l'en-tête de la colonne que vous souhaitez utiliser pour trier les événements des journaux d'exécution des tâches de Kaspersky Security for Windows Server.

Le résultat du tri est conservé jusqu'à la prochaine consultation des journaux d'exécution des tâches.

## Filtrage des événements dans les journaux d'exécution des tâches

Si vous le souhaitez, vous pouvez afficher dans la liste des événements des journaux d'exécution des tâches uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage que vous définissez (filtres).

► *Pour filtrer les événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez **Filtre**.  
La fenêtre **Paramètres du filtre** s'ouvre.
3. Pour ajouter un filtre, procédez comme suit :
  - a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez filtrer les événements.
  - b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.
  - c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.
  - d. Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.

4. Le cas échéant, réalisez une des opérations suivantes :
  - Afin de réunir quelques filtres à l'aide de l'opérateur logique "ET", sélectionnez l'option **Quand toutes les conditions sont remplies**.
  - Afin de réunir quelques filtres à l'aide de l'opérateur logique "OU", sélectionnez l'option **Quand n'importe quelle condition est remplie**.
5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements dans la liste des événements des journaux d'exécution des tâches.

La liste des événements des journaux d'exécution des tâches affiche alors uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusqu'à la prochaine consultation des journaux d'exécution des tâches.

► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez l'option **Supprimer le filtre**.

La liste des événements des journaux d'exécution des tâches reprend alors tous les événements.

## Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security for Windows Server dans les journaux d'exécution des tâches

Les journaux d'exécution des tâches reprennent des informations détaillées sur tous les événements survenus dans ces tâches depuis leur lancement jusqu'au moment de la consultation ainsi que les statistiques d'exécution des tâches et leurs paramètres.

► *Pour consulter les statistiques et les informations relatives à une tâche de Kaspersky Security for Windows Server, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le volet résultats, ouvrez la fenêtre **Journaux** à l'aide d'une des méthodes suivantes :
  - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.
  - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal et choisissez l'option **Voir le journal**.
4. La fenêtre qui s'ouvre affiche les informations suivantes :
  - L'onglet **Statistiques** indique l'heure de lancement et de fin de la tâche et ses statistiques ;
  - L'onglet **Événements** présente la liste des événements consignés pendant l'exécution de la tâche ;
  - L'onglet **Options** reprend les paramètres de la tâche.
5. Le cas échéant, cliquez sur le bouton **Filtre** pour filtrer les événements dans le journal d'exécution de la tâche.
6. Le cas échéant, cliquez sur le bouton **Exporter** pour exporter les données du journal d'exécution de la tâche dans un fichier au format CSV ou TXT.

7. Cliquez sur le bouton **Fermer**.

La fenêtre **Journaux** se ferme.

## Exportation des informations depuis le journal d'exécution de la tâche

Vous pouvez exporter les données contenues dans le journal d'exécution de la tâche dans un fichier au format CSV ou TXT.

► *Pour exporter les données du journal d'exécution de la tâche, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le volet résultats, ouvrez la fenêtre **Journaux** à l'aide d'une des méthodes suivantes :
  - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.
  - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal et choisissez l'option **Voir le journal**.
4. Dans la partie inférieure de la fenêtre **Journaux**, cliquez sur le bouton **Exporter**.  
La fenêtre **Enregistrer sous** s'ouvre.
5. Indiquez le nom, l'emplacement et le type d'encodage dans lequel vous souhaitez exporter les informations du journal d'exécution de la tâche.
6. Cliquez sur le bouton **Enregistrer**.

Les paramètres définis seront enregistrés.

## Suppression des événements des journaux d'exécution des tâches

Par défaut, Kaspersky Security for Windows Server conserve les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez supprimer manuellement tous les événements des journaux d'exécution des tâches terminées à ce moment.

Les événements des journaux des tâches en cours d'exécution et les journaux utilisés par d'autres utilisateurs ne seront pas supprimés.

► *Pour supprimer des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Exécutez une des actions suivantes :
  - Si vous souhaitez supprimer des événements de tous les journaux d'exécution des tâches terminées en ce moment, ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez l'option **Effacer**.

- Si vous souhaitez effacer le journal d'une tâche distincte, ouvrez, dans le panneau de détails, le menu contextuel d'un événement survenu dans la tâche dont vous souhaitez effacer le journal et choisissez **Supprimer**.
- Si vous souhaitez effacer le contenu des journaux d'exécution de plusieurs tâches, procédez comme suit :
  - a. Dans le panneau de détails, utilisez la touche **Ctrl** ou **Maj** pour sélectionner les événements survenus dans les tâches dont vous souhaitez supprimer les journaux.
  - b. Ouvrez le menu contextuel du menu de n'importe lequel des événements enregistrés et choisissez l'option **Supprimer**.
- 4. Dans la fenêtre de confirmation de la suppression, cliquez sur **Oui** afin de confirmer la suppression de la clé.

Les journaux d'exécution des tâches sélectionnés seront effacés. La suppression des événements des journaux d'exécution des tâches sera enregistrée dans le journal d'audit système.

## Journaux de sécurité

Kaspersky Security for Windows Server tient un journal des événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le serveur protégé. Ce journal enregistre les événements suivants :

- Événements de Protection contre les exploits.
- Les événements critiques du composant Inspection des journaux.
- Les événements critiques qui indiquent une tentative de violation de la sécurité (pour les tâches Protection en temps réel du serveur, Analyse à la demande, Moniteur d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez purger les journaux de sécurité de la même manière que pour le journal d'audit système (cf. section "Suppression d'événements du journal d'audit système" à la page [216](#)). Dans ce cas, Kaspersky Security for Windows Server enregistre l'événement d'audit système sur la purge des Journaux de sécurité.

## Consultation du journal des événements de Kaspersky Security for Windows Server dans l'observateur d'événements

Le composant logiciel enfichable Observateur d'événements pour Microsoft Management Console permet de consulter le journal des événements de Kaspersky Security for Windows Server. Kaspersky Security for Windows Server y consigne les événements nécessaires au diagnostic des échecs de fonctionnement de l'application.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements selon les critères suivants :

- **Selon le type d'événement**
- **Selon le niveau de détail.** Le niveau de détail correspond au niveau d'importance des événements enregistrés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est Événements d'information : les événements de tous les niveaux d'importance sont consignés ; le moins détaillé est le niveau Événements critiques 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 Événements importants (seuls les événements importants et critiques sont enregistrés) ; pour le composant Mise à jour, c'est le niveau Événements d'information qui est sélectionné.

► *Pour consulter les informations reprises dans le journal des événements de Kaspersky Security for*

*Windows Server.*

1. Cliquez sur le bouton **Démarrer**, saisissez la commande `mmc` dans la barre de recherche, puis appuyez sur la touche **ENTER**.  
La fenêtre de Microsoft Management Console s'ouvre.
2. Choisissez **Fichier > Ajouter ou supprimer un composant logiciel enfichable**.  
La fenêtre **Ajout et suppression de composants logiciels enfichables** s'ouvre.
3. Dans la liste des composants logiciels enfichables disponibles, sélectionnez **Observateur d'événements** et cliquez sur le bouton **Ajouter**.  
La fenêtre **Sélection d'ordinateur** s'ouvre.
4. Indiquez dans la fenêtre **Sélection d'ordinateur** l'ordinateur sur lequel Kaspersky Security for Windows Server est installé, puis cliquez sur le bouton **OK**.
5. Dans la fenêtre **Ajout et suppression de composants logiciels enfichables**, cliquez sur le bouton **OK**.  
Le nœud **Observateur d'événements** apparaît dans l'arborescence de Microsoft Management Console.
6. Développez le nœud **Observateur d'événements** et sélectionnez le nœud enfant **Journaux des applications et des services > Kaspersky Security for Windows Server**.  
Le journal des événements de Kaspersky Security for Windows Server s'ouvre.

## Configuration des paramètres des journaux dans la console de Kaspersky Security for Windows Server

Vous pouvez configurer les paramètres suivants pour les journaux de Kaspersky Security for Windows Server :

- Durée de la conservation des événements dans les journaux d'exécution des tâches et du journal d'audit système ;
  - Emplacement du dossier dans lequel Kaspersky Security for Windows Server enregistre les fichiers des journaux d'exécution des tâches et du journal d'audit système.
  - Seuils de déclenchement des événements *Les bases de l'application sont dépassées*, *Les bases de l'application sont fortement dépassées* et *Analyse des zones critiques non réalisée depuis longtemps* ;
  - Événements consignés par Kaspersky Security for Windows Server dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements de Kaspersky Security for Windows Server dans la console Observateur d'événements.
  - Paramètres de la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le serveur syslog.
- *Pour configurer les journaux de Kaspersky Security for Windows Server, procédez comme suit :*
1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications** et choisissez l'option **Propriétés**.  
La fenêtre **Paramètres des journaux et notifications** s'ouvre.
  2. Dans la fenêtre **Paramètres des journaux et des notifications**, configurez les journaux en fonction de vos exigences. Pour ce faire, procédez comme suit :
    - Sous l'onglet **Général**, sélectionnez, le cas échéant, les événements consignés par Kaspersky Security

for Windows Server dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements de Kaspersky Security for Windows Server dans la console Observateur d'événements. Pour ce faire, procédez comme suit :

- Dans la liste **Composant**, sélectionnez le composant de Kaspersky Security for Windows Server pour lequel vous souhaitez indiquer le niveau de détails.

Pour les composants Protection des fichiers en temps réel, Protection RPC des stockages réseau connectés, Protection ICAP des stockages réseau connectés, Monitoring des scripts, Analyse à la demande et Mise à jour, il est prévu de consigner les événements dans les journaux d'exécution des tâches et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Journal d'exécution de la tâche** et **Journal des événements Windows**. Pour les composants Quarantaine et Sauvegarde, les événements sont enregistrés dans le journal d'audit système et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Audit** et **Journal des événements Windows**.

- La liste **Niveau d'importance** permet de sélectionner le niveau de détail des événements dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements pour le composant fonctionnel sélectionné.  
Le tableau de la liste des événements en dessous reprend des cases cochées en regard des événements consignés dans les journaux d'exécution des tâches, le journal d'audit système et le journal des événements en fonction du niveau de détail sélectionné.
- Si vous souhaitez activer manuellement l'enregistrement d'événements distincts pour le module fonctionnel sélectionné, procédez comme suit :
  - a. Dans la liste **Niveau d'importance**, choisissez **Personnalisé**.
  - b. Dans le tableau de la liste des événements, cochez les cases en regard des événements dont vous souhaitez activer l'enregistrement dans les journaux d'exécution des tâches, le journal d'audit système et le journal des événements
- Sous l'onglet **Avancé**, configurez les paramètres de stockage des journaux et les seuils de création des événements sur l'état de la protection du serveur :
  - Dans la section **Stockage des journaux** :
    - **Dossier des journaux**  
Chemin d'accès au dossier contenant les journaux, au format UNC (Universal Naming Convention).  
Chemin par défaut : C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\  
En cas de modification du chemin par défaut, un dossier portant le nom correspondant est créé. Le nouveau journal est stocké dans le nouveau dossier. Les anciens journaux sont conservés.
    - **Supprimer les journaux d'exécution de la tâche de plus de (jours)**  
La case active ou désactive la fonction qui supprime les journaux contenant les résultats de l'exécution des tâches terminées et les événements publiés dans les journaux des tâches en cours d'exécution à l'issue de la période définie (par défaut : 30 jours).  
Si la case est cochée, Kaspersky Security for Windows Server supprime les journaux des résultats d'exécution des tâches terminées et les événements publiés dans les journaux



d'exécution des tâches à l'issue de la période définie.

Cette case est cochée par défaut.

- **Supprimer les événements du journal d'audit système de plus de (jours)**

La case active ou désactive la fonction qui supprime les événements enregistrés dans le journal d'audit système à l'issue de la période définie (par défaut : 60 jours).

Si la case est cochée, Kaspersky Security for Windows Server supprime les événements enregistrés dans le journal d'audit système à l'issue de la période définie.

Cette case est décochée par défaut.

- Dans la section **Seuils de déclenchement des événements** :

- Nombre de jours à l'issue desquels les événements *Les bases de l'application sont dépassées*, *Les bases de l'application sont fortement dépassées* et *Analyse des zones critiques non réalisée depuis longtemps* sont déclenchés.

Tableau 36. Seuils de déclenchement des événements.

Paramètre	Seuils de déclenchement des événements.
Description	Vous pouvez définir le seuil de déclenchement des événements des types suivants : <i>Les bases de l'application sont dépassées</i> et <i>Les bases de l'application sont fortement dépassées</i> . Cet événement se déclenche lorsque les bases de Kaspersky Security for Windows Server n'ont pas été actualisées durant une période (nombre de jours) définie depuis la date de publication des mises à jour des bases de données installées dernièrement. Vous pouvez configurer la notification de l'administrateur lorsque ces événements surviennent.  <i>Analyse des zones critiques non réalisée depuis longtemps</i> . Cet événement se déclenche si aucune des tâches accompagnées de la case <b>Considérer l'exécution de la tâche comme une analyse des zones critiques</b> n'a été exécutée au cours du nombre de jours indiqué.
Valeurs possibles	Nombre de jours compris entre 1 et 365
Valeur par défaut	Les bases de l'application sont dépassées : 7 jours. Les bases de l'application sont dépassées : 14 jours. Analyse des zones critiques non réalisée depuis longtemps : 30 jours.

- Sous l'onglet **Intégration à SIEM**, configurez les paramètres de la publication des événements de l'audit et des événements des tâches exécutées sur le serveur syslog (cf. section "Configuration des paramètres d'intégration à SIEM" à la page [224](#)).

3. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

## Dans cette section

A propos de l'intégration à SIEM .....	<a href="#">224</a>
Configuration des paramètres d'intégration à SIEM .....	<a href="#">224</a>

## A propos de l'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des volumes des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il récolte et analyse les événements reçus et réalise également d'autres actions d'administration des journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : ce mode suppose que tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'ordinateur local même après avoir été envoyés à SIEM. Il est recommandé d'utiliser ce mode pour réduire au maximum la charge sur le serveur protégé.
- Supprimer les copies locales des événements : ce mode suppose que tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans SIEM soient supprimés de l'ordinateur local.

L'application ne supprime jamais les versions locales des Journaux de sécurité.

Kaspersky Security for Windows Server peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus par le SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Il est recommandé de choisir le format des événements d'après la configuration du SIEM utilisé.

### Paramètres de fiabilité

Vous pouvez réduire le risque d'erreur d'envoi des événements à SIEM en indiquant les paramètres de connexion au serveur syslog de miroir.

Le serveur syslog de miroir est un serveur syslog complémentaire vers lequel l'application passe automatiquement si la connexion au serveur principal syslog ou son utilisation sont impossibles.

Kaspersky Security for Windows Server vous informe également d'une tentative manquée de connexion à SIEM et des erreurs d'envoi des événements à SIEM à l'aide des événements de l'audit système.

## Configuration des paramètres d'intégration à SIEM

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres de fonctionnement (cf. tableau ci-dessous).

Tableau 37. Paramètres d'intégration à SIEM

Paramètre	Valeur par défaut	Description
<b>Envoyer les événements à un serveur syslog externe via le protocole syslog</b>	Pas appliqué	Vous pouvez activer et désactiver l'intégration à SIEM en cochant ou décochant la case.
<b>Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe</b>	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi à SIEM en cochant ou décochant la case.

<b>Format des événements</b>	Données structurées	Vous pouvez choisir un de deux formats sous lesquels l'application convertit les événements avant de les envoyer au serveur syslog pour mieux les reconnaître au niveau du SIEM.
<b>Protocole de connexion</b>	TCP	Vous pouvez configurer la connexion aux serveurs syslog principal et complémentaire via les protocoles UDP ou TCP à l'aide de la liste déroulante.
<b>Paramètres de connexion au serveur syslog principal</b>	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.
<b>Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible</b>	Pas appliqué	Vous pouvez activer et désactiver l'application du serveur syslog de miroir à l'aide de la case.
<b>Paramètres de connexion au serveur syslog complémentaire</b>	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog complémentaire à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.

► *Pour configurer les paramètres d'intégration à SIEM, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Choisissez l'option **Propriétés**.  
La fenêtre **Paramètres des journaux et notifications** s'ouvre.
3. Sélectionnez l'onglet **Intégration à SIEM**.
4. Dans la section **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.

La case active ou désactive l'utilisation de la fonction d'envoi des événements publiés au serveur syslog externe.

Si la case est cochée, l'application exécute l'envoi des événements publiés sur SIEM conformément à la configuration des paramètres d'intégration à SIEM.

Si la case est décochée, l'application n'exécute pas l'intégration à SIEM. Vous ne pouvez pas configurer les paramètres d'intégration à SIEM si la case est décochée.

Cette case est décochée par défaut.

5. Si besoin, dans la section **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe**.

La case active ou désactive la suppression des copies locales des journaux au moment de leur envoi à SIEM.

Si la case est cochée, l'application supprime les copies locales des événements une fois

publiées dans le SIEM. Il est recommandé d'utiliser ce mode sur les ordinateurs de faible puissance.

Si la case est décochée, l'application envoie uniquement les événements à SIEM. Les copies des journaux continuent d'être conservées localement.

Cette case est décochée par défaut.

L'état de la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe** n'influence pas les paramètres de conservation des événements des Journaux de sécurité : l'application ne supprime jamais automatiquement les événement des Journaux de sécurité.

6. Dans la section **Format des événements**, indiquez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi à SIEM.

Par défaut, l'application exécute la conversion au format de données structurées.

7. Dans la section **Paramètres de connexion**, procédez comme suit :
  - Indiquez le protocole de connexion à SIEM.
  - Indiquez les paramètres de connexion au serveur syslog principal.  
Vous pouvez indiquer l'adresse IP uniquement au format IPv4.
  - Cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si vous voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n'est pas possible.
    - Définissez les paramètres suivants de connexion au serveur syslog de miroir : **Adresse IP** et **Port**.  
Les champs **Adresse IP** et **Port** pour le serveur syslog de miroir ne peuvent pas être modifiés si la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible** est décochée.  
Vous pouvez indiquer l'adresse IP uniquement au format IPv4.
8. Cliquez sur le bouton **OK**.  
Les paramètres d'intégration à SIEM configurés seront appliqués.

## Configuration des notifications

Cette section contient des informations sur les différentes méthodes de notification des utilisateurs et des administrateurs de Kaspersky Security for Windows Server sur les événements de l'application et l'état de la protection du serveur, ainsi que les instructions relatives à la configuration des notifications.

### Contenu du chapitre

Moyens de notification de l'administrateur et des utilisateurs .....	<a href="#">227</a>
Configuration des notifications de l'administrateur et des utilisateurs .....	<a href="#">228</a>

## Moyens de notification de l'administrateur et des utilisateurs

Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au serveur protégé sur les événements liés au fonctionnement de Kaspersky Security for Windows Server et à l'état de la protection antivirus du serveur.

L'application assure l'exécution des tâches suivantes :

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent le serveur protégé et les utilisateurs de terminaux du serveur peuvent obtenir des informations sur les événements de type *Objet détecté* qui surviennent pendant la tâche Protection des fichiers en temps réel.

Dans la console de l'application, vous pouvez activer les notifications de l'administrateur ou des utilisateurs de plusieurs manières :

- Moyens de notification des utilisateurs :
  - a. Outils des services des terminaux.  
Vous pouvez utiliser cette méthode pour la notification des utilisateurs du serveur de terminal si le serveur protégé est un serveur de terminaux.
  - b. Outils du service Windows Messenger.  
Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger. Ce mode n'est pas pris en charge si le serveur protégé tourne sous Microsoft Windows Server 2008 ou suivant
- Moyens de notification des administrateurs :
  - a. Outils du service Windows Messenger.  
Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger. Ce mode n'est pas pris en charge si le serveur protégé tourne sous Microsoft Windows Server 2008 ou suivant
  - b. Lancement du fichier exécutable.  
Cette méthode lance un fichier exécutable stocké sur le disque local du serveur protégé en fonction de l'événement.
  - c. Envoi par email.  
Ce mode permet l'envoi d'emails.

Vous pouvez créer un texte différent pour chaque type d'événement. Ce texte peut contenir des champs avec les informations sur l'événement. Un texte prédéfini du message est utilisé par défaut pour les notifications des utilisateurs.

## Configuration des notifications de l'administrateur et des utilisateurs

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, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications** et choisissez l'option **Propriétés**.

La fenêtre **Paramètres des journaux et notifications** s'ouvre.

2. Sous l'onglet **Notifications**, indiquez les modes de notification :
  - a. Dans la liste **Type d'événement**, sélectionnez les types d'événements.
  - b. Dans le groupe de paramètres **Informez les administrateurs** ou **Informez les utilisateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

Vous pouvez configurer les notifications des utilisateurs uniquement pour les événements **Objet détecté**, **Stockage de masse douteux détecté et restreint** et **Hôte ajouté à la liste des ordinateurs bloqués**.

3. Si vous souhaitez modifier le texte de la notification, procédez comme suit :
  - a. Cliquez sur le bouton **Texte du message**.
  - b. Dans la fenêtre qui s'ouvre, saisissez le texte qui sera affiché dans le message relatif à l'événement.

Vous pouvez créer un texte de message unique pour plusieurs types d'événements : après avoir choisi le mode de notification pour un type d'événement, sélectionnez, à l'aide de la touche **Ctrl** ou **Maj**, les autres types d'événements pour lesquels vous souhaitez utiliser ce même texte de message avant de cliquer sur le bouton **Texte du message**.

- c. Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Macro** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.
  - d. Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur **Par défaut**.
4. Si vous souhaitez configurer les modes de notification de l'administrateur sur l'événement sélectionnés, ouvrez l'onglet **Notification**, cliquez sur le bouton **Configuration** dans la section **Informez les administrateurs** et procédez à la configuration des modes sélectionnés dans la fenêtre **Paramètres avancés**. Pour ce faire, procédez comme suit :
  - a. Pour les notifications via email, ouvrez l'onglet **Email** et saisissez les adresses email des destinataires (séparez les adresses par un point-virgule), le nom ou l'adresse de réseau du serveur SMTP, ainsi que son port, dans les champs prévus à cet effet. Si nécessaire, indiquez le texte qui figurera dans les champs **Objet** et **De**. Le texte du champ **Objet** peut contenir des variables de champs d'informations

(cf. tableau ci-dessous).

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 cocher la case **Utiliser l'authentification SMTP** dans le groupe **Paramètres d'authentification** et saisir le nom et le mot de passe de l'utilisateur dont l'authenticité sera vérifiée.

- b. Pour les notifications via **Service Windows Messenger**, sous l'onglet **Service Windows Messenger**, composez la liste des ordinateurs des destinataires des messages : pour chaque ordinateur que vous souhaitez ajouter, cliquez sur le bouton **Ajouter** et dans le champ, saisissez son nom de réseau.

N'oubliez pas que les notifications via le Service Windows Messenger ne sont pas utilisées si le serveur protégé tourne sous Microsoft Windows Server 2008 et les versions suivantes de Microsoft Windows Server.

- c. 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** 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.

En indiquant le chemin d'accès au fichier exécutable, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Si vous souhaitez limiter le nombre de messages de notification en fonction d'événements d'un même type par unité de temps, cochez la case **Ne pas envoyer la même notification plus de** sous l'onglet **Avancé** et indiquez la valeur souhaitée par unité de temps.

- 5. Cliquez sur le bouton **OK**.

Les paramètres de la notification définis seront enregistrés.

Tableau 38. Champs d'information sur les événements

Variable	Description
%EVENT_TYPE%	Type d'événements.
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%EVENT_SEVERITY%	Niveau d'importance de l'événement.
%OBJECT%	Nom de l'objet (dans les tâches Protection en temps réel du serveur et Analyse à la demande) Dans la tâche de 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.
%VIRUS_NAME%	Nom de l'objet détecté selon la classification de l'Encyclopédie des virus <a href="https://encyclopedia.kaspersky.com/knowledge/classification/">https://encyclopedia.kaspersky.com/knowledge/classification/</a> . Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Security for Windows Server renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche (cf. section "Consultation des statistiques et des informations relatives à une tâche de Kaspersky Security for Windows Server dans les journaux d'exécution des tâches" à la page 218).



Variable	Description
%VIRUS_TYPE%	Type de l'objet détecté selon la classification de Kaspersky Lab, par exemple "virus" ou "cheval de Troie". Figure dans le nom complet de l'objet détecté renvoyé par Kaspersky Security for Windows Server lorsque celui-ci considère l'objet comme infecté ou probablement infecté. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
%USER_COMPUTER%	Dans les tâches Protection des fichiers en temps réel et Protection RPC des stockages réseau connectés, nom d'ordinateur de l'utilisateur qui a accédé à l'objet sur l'ordinateur.
%USER_NAME%	Dans les tâches Protection des fichiers en temps réel et Protection RPC des stockages réseau connectés, désigne le nom de l'utilisateur qui a sollicité l'objet sur le serveur.
%FROM_COMPUTER%	Nom du serveur protégé d'où provient la notification
%EVENT_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)

# Lancement et arrêt de Kaspersky Security for Windows Server

Cette section fournit des informations sur le lancement de la console de l'application, ainsi que sur le lancement et l'arrêt du service Kaspersky Security.

## Contenu du chapitre

Lancement et arrêt du plug-in d'administration de Kaspersky Security for Windows Server .....	<a href="#">231</a>
Lancement de la console de Kaspersky Security for Windows Server depuis le menu Démarrer .....	<a href="#">231</a>
Lancement et arrêt du service Kaspersky Security .....	<a href="#">232</a>
Lancement des composants Kaspersky Security for Windows Server en mode sans échec du système d'exploitation .....	<a href="#">234</a>

## Lancement et arrêt du plug-in d'administration de Kaspersky Security for Windows Server

Aucune action supplémentaire n'est requise pour lancer le plug-in d'administration de Kaspersky Security for Windows Server dans Kaspersky Security Center. Après l'installation du plug-in sur l'ordinateur de l'administrateur, le lancement s'opère en même temps que le lancement de Kaspersky Security Center. Vous trouverez toutes les informations détaillées sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

## Lancement de la console de Kaspersky Security for Windows Server depuis le menu Démarrer

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

► *Pour démarrer la console de l'application depuis le menu **Démarrer** :*

1. Dans le menu **Démarrer**, sélectionnez **Programmes > Kaspersky Security for Windows Server > Outils d'administration > Console de Kaspersky Security for Windows Server**.

Pour ajouter d'autres composants logiciels enfichables à la console de l'application, lancez-la en mode auteur.

► *Pour lancer la console de l'application en mode auteur, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez **Programmes > Kaspersky Security for Windows Server > Outils d'administration**.
2. Dans le menu contextuel de la console de l'application, choisissez la commande **Auteur**.

La console de l'application est lancée en mode auteur.

Si vous avez lancé la console de l'application sur le serveur protégé, la fenêtre de la console de l'application s'ouvre.

Si vous avez lancé la console de l'application non pas sur le serveur protégé, mais sur un autre ordinateur, connectez-vous au serveur protégé.

► *Pour vous connecter au serveur à protéger, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Sélectionnez la commande **Se connecter à un autre ordinateur**.  
La fenêtre **Sélection d'ordinateur** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez **Autre ordinateur**.
4. Dans le champ de saisie de droite, indiquez le nom réseau du serveur à protéger.
5. Cliquez sur le bouton **OK**.

La console de l'application est connectée au serveur protégé.

Si le compte utilisateur employé pour accéder à Microsoft Windows ne dispose pas des privilèges d'accès au service Kaspersky Security Management sur l'ordinateur, cochez la case **Se connecter sous le compte utilisateur** et indiquez un autre compte utilisateur qui dispose de tels privilèges.

## Lancement et arrêt du service Kaspersky Security

Le Service Kaspersky Security est lancé automatiquement par défaut immédiatement après le démarrage du système d'exploitation. Le service Kaspersky Security gère les processus de travail chargés des tâches Protection en temps réel du serveur, Contrôle du serveur, Analyse à la demande et de la mise à jour.

Le lancement de Kaspersky Security for Windows Server marque par défaut le lancement des tâches Protection des fichiers en temps réel, Monitoring des scripts (si ce module est installé) et Analyse au démarrage du système d'exploitation ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Si vous arrêtez le Service Kaspersky Security, l'ensemble des tâches en cours d'exécution sera interrompu. Après que vous avez relancé le service Kaspersky Security, l'application lance automatiquement uniquement les tâches dont la planification reprend la fréquence **Au lancement de l'application**, les autres tâches sont lancées manuellement.

Vous pouvez lancer et arrêter le service Kaspersky Security à l'aide du menu contextuel du nœud **Kaspersky Security** ou via le composant logiciel enfichable Microsoft Windows Services.

**Vous pouvez lancer et arrêter Kaspersky Security for Windows Server uniquement si vous faites partie du groupe d'administrateurs sur le serveur protégé.**

► *Pour arrêter ou lancer l'application via la console de l'application, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.

2. Choisissez une des commandes suivantes :

- **Arrêter le service.**
- **Lancer le service.**

Le Service Kaspersky Security sera lancé ou arrêté.

## Lancement des composants Kaspersky Security for Windows Server en mode sans échec du système d'exploitation

Cette section fournit des informations sur l'utilisation de Kaspersky Security for Windows Server en mode sans échec.

### Contenu du chapitre

A propos de l'utilisation de Kaspersky Security for Windows Server en mode sans échec du système d'exploitation .....	<a href="#">234</a>
Lancement de Kaspersky Security for Windows Server en mode sans échec .....	<a href="#">235</a>

## A propos de l'utilisation de Kaspersky Security for Windows Server en mode sans échec du système d'exploitation

Les composants de Kaspersky Security for Windows Server peuvent être démarrés lors du chargement du système d'exploitation en mode sans échec. En plus de Kaspersky Security Service (kavfs.exe), le pilote klam.sys est chargé et utilisé pour l'enregistrement du service Kaspersky Security en tant que service protégé au démarrage du système d'exploitation. Pour en savoir plus, cf. section Enregistrement du Service Kaspersky Security comme service protégé.

Kaspersky Security for Windows Server peut être démarré dans les modes sans échec suivants du système d'exploitation :

- Mode minimal sans échec : ce mode est lancé lorsque l'option standard du mode sans échec du système d'exploitation est sélectionnée. Dans ce cas, Kaspersky Security for Windows Server peut démarrer les composants suivants :
  - Protection des fichiers en temps réel.
  - Analyse à la demande.
  - Contrôle du lancement des applications et Génération des règles du Contrôle du lancement des applications.
  - Inspection des journaux.
  - Moniteur d'intégrité des fichiers.
  - Vérification de l'intégrité de l'application.
  - Protection contre le chiffrement.
  - Stockage des ordinateurs bloqués.
- Réseau mode sans échec : ce mode est lancé lorsque le système d'exploitation est chargé en mode sans échec avec les pilotes réseau. En plus de démarrer les composants en mode sans échec minimal, Kaspersky Security for Windows Server peut démarrer les composants suivants :
  - Mise à jour des bases de données.

- Mise à jour des modules de l'application.
- Protection des stockages réseau.

## Lancement de Kaspersky Security for Windows Server en mode sans échec

Par défaut, Kaspersky Security for Windows Server ne démarre pas en mode sans échec lors du chargement du système d'exploitation.

► *Pour que Kaspersky Security for Windows Server démarre en mode sans échec du système d'exploitation, procédez comme suit :*

1. Démarrez l'éditeur de registre Windows (C:\Windows\regedit.exe).
2. Ouvrez la clé du registre du système [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Ouvrez le paramètre LoadInSafeMode.
4. Définissez la valeur 1.
5. Cliquez sur le bouton **OK**.

► *Pour annuler le démarrage de Kaspersky Security for Windows Server en mode sans échec du système d'exploitation, procédez comme suit :*

1. Démarrez l'éditeur de registre Windows (C:\Windows\regedit.exe).
2. Ouvrez la clé du registre du système [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Ouvrez le paramètre LoadInSafeMode.
4. Définissez la valeur 0.
5. Cliquez sur le bouton **OK**.

# Auto-défense de Kaspersky Security for Windows Server

Cette section contient des informations sur les mécanismes d'auto-défense de Kaspersky Security for Windows Server.

## Contenu du chapitre

A propos de l'auto-défense de Kaspersky Security for Windows Server .....	<a href="#">236</a>
Protection contre les modifications des dossiers avec les composants Kaspersky Security for Windows Server installés .....	<a href="#">236</a>
Protection contre les modifications des clés de registre de Kaspersky Security for Windows Server .....	<a href="#">236</a>
Enregistrement du service Kaspersky Security en tant que service protégé .....	<a href="#">237</a>
Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server .....	<a href="#">239</a>

## A propos de l'auto-défense de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server comprend des mécanismes d'auto-défense qui protègent l'application contre la modification ou la suppression de ses dossiers sur le disque dur, les processus de mémoire, et les entrées du registre du système.

## Protection contre les modifications des dossiers avec les composants Kaspersky Security for Windows Server installés

Kaspersky Security for Windows Server limite le renommage et la suppression des dossiers des composants de l'application installés et correspondant à un compte utilisateur. Par défaut, les chemins d'accès aux dossiers d'installation de l'application sont les suivants :

- Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\
- Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\

## Protection contre les modifications des clés de registre de Kaspersky Security for Windows Server

Kaspersky Security for Windows Server limite les droits d'accès aux branches et clés de registre suivants qui



assurent le chargement des pilotes et services de l'application :

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslpl]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klelam]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump] (sur la version 64 bits de Microsoft Windows)
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\Trace]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Trace] (sur la version 64 bits de Microsoft Windows)

Les droits de modification de ces branches et clés de registre sont accordés au compte Local System (SYSTEM) uniquement. Les comptes Utilisateur et Administrateur se voient accorder des droits de lecture seule.

## Enregistrement du service Kaspersky Security en tant que service protégé

La technologie *Protected Process Light* (également appelée "PPL") fait en sorte que le système d'exploitation charge uniquement les services et les processus de confiance. Pour qu'un service puisse fonctionner comme un service protégé, un pilote à *lancement anticipé anti-application malveillante* doit être installé sur le serveur protégé.

Un pilote à *lancement anticipé anti-application malveillante* (également appelé "ELAM") fournit une protection aux serveurs de votre réseau lors de leur démarrage et avant l'initialisation des pilotes tiers.

Le pilote ELAM est automatiquement installé lors de l'installation de Kaspersky Security for Windows Server et sert à enregistrer le service Kaspersky Security comme PPL lors du démarrage du système d'exploitation. Lorsque le service Kaspersky Security (KAVFS) est démarré en tant que processus protégé par le système, d'autres processus non protégés sur le système ne peuvent pas injecter de threads, écrire dans la mémoire virtuelle du processus protégé ou arrêter le service.

Quand un processus est lancé en tant que PPL, l'utilisateur ne peut pas l'administrer en ignorant les autorisations qu'il lui ont été attribuées. L'enregistrement du service Kaspersky Security comme PPL avec le pilote ELAM est pris en charge sur les systèmes d'exploitation Microsoft Windows 2016 et suivants. Si vous installez Kaspersky Security for Windows Server sur un serveur tournant sous un système d'exploitation compatible avec PPL, l'administration des autorisations pour le service Kaspersky Security (KAVFS) ne sera pas disponible.

- *Pour installer Kaspersky Security en tant que PPL, exécutez la commande suivante :*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

# Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Security for Windows Server et des services Windows enregistré par l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

## Contenu du chapitre

A propos des autorisations d'administration de Kaspersky Security for Windows Server .....	<a href="#">239</a>
A propos des autorisations d'administration des services enregistrés .....	<a href="#">241</a>
A propos des autorisations d'administration du Service Kaspersky Security .....	<a href="#">241</a>
A propos des autorisations d'accès au Service Kaspersky Security Management.....	<a href="#">243</a>
Configuration des autorisations d'accès à l'administration de Kaspersky Security for Windows Server et au Service Kaspersky Security .....	<a href="#">244</a>
Accès protégé par mot de passe aux fonctions de Kaspersky Security for Windows Server .....	<a href="#">246</a>
Configuration des autorisations d'accès dans Kaspersky Security Center .....	<a href="#">246</a>

## A propos des autorisations d'administration de Kaspersky Security for Windows Server

Par défaut, l'accès à toutes les fonctions de Kaspersky Security for Windows Server est octroyé aux utilisateurs du groupe Administrateurs sur le serveur protégé et aux utilisateurs du groupe KAVWSEE Administrators créé sur le serveur protégé lors de l'installation de Kaspersky Security for Windows Server et aussi au groupe SYSTEM.

Les utilisateurs qui ont accès à la fonction **Modifier** les privilèges de Kaspersky Security for Windows Server peuvent offrir l'accès aux fonctions de Kaspersky Security for Windows Server 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 Security for Windows Server, il ne pourra pas ouvrir la console de l'application.

Vous pouvez attribuer à l'utilisateur ou au groupe d'utilisateurs un des niveaux prédéfinis d'accès suivants :

- **Contrôle complet** : accès à toutes les fonctions de l'application : consultation et modification des paramètres généraux de Kaspersky Security for Windows Server, des paramètres des composants, des autorisations des utilisateurs de Kaspersky Security for Windows Server ainsi que la consultation des statistiques de Kaspersky Security for Windows Server.
- **Modifier** : accès à l'ensemble des fonctions de l'application, sauf la modification des autorisations des utilisateurs : possibilité de consulter et de modifier les paramètres généraux et les paramètres des composants de Kaspersky Security for Windows Server.
- **Lire** : consultation des paramètres généraux de Kaspersky Security for Windows Server, des paramètres des composants de Kaspersky Security for Windows Server, des statistiques de Kaspersky Security for Windows Server et des autorisations d'utilisateur de Kaspersky Security for Windows Server.

Vous pouvez également configurer les autorisations d'accès avancées : autoriser ou interdire l'accès aux fonctions

spécifiques de Kaspersky Security for Windows Server.

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

Tableau 39. A propos des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server

Autorisations d'accès	Description
Administration des tâches	Lancement/arrêt/suspension/reprise d'une tâche de Kaspersky Security for Windows Server.
Création et suppression des tâches Analyse à la demande	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilités : <ul style="list-style-type: none"> <li>• Importation des paramètres de Kaspersky Security for Windows Server depuis un fichier de configuration.</li> <li>• Modifiez les paramètres de l'application.</li> </ul>
Lire les paramètres	Possibilités : <ul style="list-style-type: none"> <li>• Consultation des paramètres généraux de Kaspersky Security for Windows Server et des paramètres des tâches.</li> <li>• Exportation des paramètres de Kaspersky Security for Windows Server vers un fichier de configuration.</li> <li>• Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.</li> </ul>
Gérer les référentiels	Possibilités : <ul style="list-style-type: none"> <li>• Placement d'objets en quarantaine ;</li> <li>• Suppression d'objets de la quarantaine et de la Sauvegarde ;</li> <li>• Restauration d'objets de la quarantaine et de la Sauvegarde.</li> </ul>
Administration des journaux	Suppression des journaux d'exécution des tâches et purge du journal d'audit système.
Lecture des journaux	Possibilité de consulter les événements de l'Antivirus dans les journaux d'exécution des tâches et le journal d'audit système.
Consultation des statistiques	Consultation des statistiques de chacune des tâches de Kaspersky Security for Windows Server.
Licence de l'application	Fonction d'activation de Kaspersky Security for Windows Server.
Suppression de l'application	Fonction de désinstallation de Kaspersky Security for Windows Server.
Lecture des privilèges	Possibilité de consulter la liste des utilisateurs de Kaspersky Security for Windows Server et des privilèges d'accès de ceux-ci.
Modification des privilèges	Possibilités : <ul style="list-style-type: none"> <li>• Modifier la liste des utilisateurs qui ont accès à l'administration de l'application ;</li> <li>• Modification des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server.</li> </ul>

## A propos des autorisations d'administration des services enregistrés

Les informations détaillées sur les services Windows enregistrés et la configuration de l'accès aux services enregistrés figurent dans le *Manuel de l'administrateur de Kaspersky Security for Windows Server*.

Lors de l'installation, Kaspersky Security for Windows Server enregistre le service Kaspersky Security (KAVFS) et le service Kaspersky Security Management (KAVFSGT) sous Windows, ainsi que la protection contre les exploits de Kaspersky Security (KAVFSSLP).

L'enregistrement du service Kaspersky Security comme Protected Process Light (PPL) avec le pilote ELAM est pris en charge sur les systèmes d'exploitation Microsoft Windows 10 et suivants. Quand un processus est lancé en tant que PPL, l'utilisateur ne peut pas l'administrer en ignorant les autorisations qu'il lui ont été attribuées. Si vous installez Kaspersky Security for Windows Server sur un ordinateur tournant sous un système d'exploitation compatible avec PPL, l'administration des autorisations pour le service Kaspersky Security (KAVFS) ne sera pas disponible.

### Service Kaspersky Security Service

Par défaut, l'accès à l'administration du Service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe "Administrateurs" du serveur à protéger, ainsi qu'aux groupes système SERVICE et INTERACTIVE avec autorisation de lecture et au groupe système SYSTEM avec autorisation de lecture et d'exécution.

Les utilisateurs qui disposent d'un accès aux fonctions du niveau Modifier les privilèges (cf. section "Accès protégé par mot de passe aux fonctions de Kaspersky Security for Windows Server" à la page [246](#)) peuvent octroyer l'accès à l'administration du Service Kaspersky Security à d'autres utilisateurs enregistrés sur le serveur protégé ou appartenant au domaine.

### Service Kaspersky Security Management

Pour administrer l'application via la console de l'application installée sur un autre serveur, il faut que le compte sous les autorisations duquel la connexion à Kaspersky Security for Windows Server s'opère possède un accès complet au service Kaspersky Security Management sur le serveur protégé.

Par défaut, l'accès au service Kaspersky Security Management est octroyé aux utilisateurs du groupe Administrateurs sur le serveur protégé et aux utilisateurs du groupe KAVWSEE Administrators créé sur le serveur protégé lors de l'installation de Kaspersky Security for Windows Server.

Vous pouvez administrer le Service Kaspersky Security Management uniquement via le composant logiciel enfichable Services de Microsoft Windows.

## A propos des autorisations d'administration du Service Kaspersky Security

Lors de l'installation, Kaspersky Security for Windows Server enregistre le Service Kaspersky Security (KAVFS) dans Windows et autorise en interne le lancement des composants au lancement du système d'exploitation. Pour réduire le risque d'accès d'un tiers aux fonctions de l'application et aux paramètres de sécurité sur le serveur protégé via l'administration du service Kaspersky Security, vous pouvez limiter les autorisations d'administration du service Kaspersky Security depuis la console de l'application ou depuis le plug-in d'administration.

Par défaut, l'accès à l'administration du Service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe "Administrateurs" du serveur à protéger, ainsi qu'aux groupes système SERVICE et INTERACTIVE avec autorisation de lecture et au groupe système SYSTEM avec autorisation de lecture et d'exécution.

Il est impossible de supprimer le compte utilisateur SYSTEM ou de modifier les autorisations de ce compte. En cas de modification des autorisations du compte utilisateur SYSTEM, les autorisations maximales sont rétablies pour ce compte lors de l'enregistrement des modifications.

Les utilisateurs qui disposent d'un accès aux fonctions du niveau (cf. section "A propos des autorisations d'administration de Kaspersky Security for Windows Server" à la page [239](#)) Modification des autorisations peuvent octroyer l'accès à l'administration du Service Kaspersky Security à d'autres utilisateurs enregistrés sur le serveur protégé ou appartenant au domaine.

Vous pouvez attribuer à l'utilisateur ou à un groupe d'utilisateurs de Kaspersky Security for Windows Server un des niveaux prédéfinis d'administration du Service Kaspersky Security :

- **Contrôle complet** : consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs, ainsi lancement et arrêt du Service Kaspersky Security.
- **Lire** : consultation des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
- **Modifier** : consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
- **Exécution** : lancement et arrêt du fonctionnement du service Kaspersky Security.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès : autoriser ou interdire l'accès à des fonctions particulières de Kaspersky Security for Windows Server (voir tableau ci-dessous).

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

Tableau 40. Restriction des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server

Fonction	Description
Lecture des paramètres du service	Consultation des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
Solliciter l'état du service auprès du Gestionnaire de contrôle des services	Interrogation sur l'état d'exécution du Service Kaspersky Security dans le gestionnaire de services de Microsoft Windows.
Interrogation du service sur son état	Interrogation du Service Kaspersky Security sur l'état de l'exécution du service.
Lire la liste des services dépendants	Consultation de la liste des services dont dépend du service Kaspersky Security ainsi et qui dépendent du service Kaspersky Security.
Modification des paramètres du service	Consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
Lancer le service	Exécution du service Kaspersky Security.

Fonction	Description
Arrêter le service	Arrêt du service Kaspersky Security.
Suspension/reprise du service	Suspension et reprise de l'exécution du service Kaspersky Security.
Lecture des privilèges	Consultation de la liste des utilisateurs du service Kaspersky Security et des privilèges d'accès de chacun d'entre eux.
Modification des privilèges	Possibilités : <ul style="list-style-type: none"> <li>• Ajout et suppression d'utilisateurs du Service Kaspersky Security ;</li> <li>• Modification des autorisations d'accès des utilisateurs au service Kaspersky Security.</li> </ul>
Suppression du service	Annulation de l'enregistrement du Service Kaspersky Security dans le Gestionnaire de service de Microsoft Windows.
Interrogations personnalisées adressées au service	Création et envoi d'interrogations personnalisées adressées au service Kaspersky Security.

## A propos des autorisations d'accès au Service Kaspersky Security Management

[Vous pouvez passer en revue la liste des services de Kaspersky Security for Windows Server.](#)

Lors de l'installation, Kaspersky Security for Windows Server enregistre le Service Kaspersky Security Management (KAVFSGT). Pour administrer l'application via la Console de l'application installée sur un autre ordinateur, il faut que le compte sous les autorisations duquel la connexion à Kaspersky Security for Windows Server s'opère possède un accès complet au service Kaspersky Security Management sur le serveur protégé.

Par défaut, l'accès au service Kaspersky Security Management est octroyé aux utilisateurs du groupe Administrateurs sur le serveur protégé et aux utilisateurs du groupe KAVWSEE Administrators créé sur le serveur protégé lors de l'installation de Kaspersky Security for Windows Server.

Vous pouvez administrer le Service Kaspersky Security Management uniquement via le composant logiciel enfichable Services de Microsoft Windows.

**Il est impossible d'autoriser ou d'interdire l'accès de l'utilisateur au Service Kaspersky Security Management en configurant Kaspersky Security for Windows Server.**

**Vous pouvez vous connecter à Kaspersky Security for Windows Server sous un compte utilisateur local si un compte utilisateur avec le même nom d'utilisateur et le même mot de passe est enregistré sur le serveur protégé.**



## Configuration des autorisations d'accès à l'administration de Kaspersky Security for Windows Server et au Service Kaspersky Security

Vous pouvez modifier la liste des utilisateurs et groupes d'utilisateurs ayant accès aux fonctions de Kaspersky Security for Windows Server et à l'administration du Service Kaspersky Security, ainsi que modifier les privilèges d'accès des utilisateurs et groupes d'utilisateurs.

► *Pour ajouter un utilisateur ou un groupe à la liste ou pour l'en supprimer, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security** et réalisez une des actions suivantes :
  - Choisissez l'option **Modifier les droits de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration des fonctions de Kaspersky Security for Windows Server.
  - Choisissez l'option **Modifier les droits d'utilisateurs pour l'administration de Service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du service Kaspersky Security.

La fenêtre **Autorisations pour Kaspersky Security** s'ouvre.

2. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
  - Pour ajouter un utilisateur ou un groupe à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe.
  - Pour supprimer un utilisateur (un groupe) de la liste, sélectionnez les utilisateurs (les groupes), puis cliquez sur le bouton **Supprimer**.
3. Cliquez sur le bouton **Appliquer**.

Les utilisateurs (ou groupes) sélectionnés seront ajoutés ou supprimés.

► *Pour modifier les autorisations d'administration de Kaspersky Security for Windows Server ou du Service Kaspersky Security d'un utilisateur ou d'un groupe d'utilisateurs, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security** et réalisez une des actions suivantes :
  - Choisissez l'option **Modifier les droits de l'utilisateur pour l'administration de l'application** si vous souhaitez configurer les autorisations d'accès aux fonctions de Kaspersky Security for Windows Server.
  - Choisissez l'option **Modifier les droits d'utilisateurs pour l'administration de Service Kaspersky Security** si vous souhaitez configurer les autorisations d'accès au Service Kaspersky Security.

La fenêtre **Autorisations pour Kaspersky Security** s'ouvre.

2. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste **Groupe ou noms d'utilisateur** l'utilisateur ou le groupe d'utilisateurs dont vous souhaitez modifier les autorisations.
3. Dans la section **Autorisation pour le groupe** « <Utilisateur (Groupe)> », cochez les cases **Autoriser** ou **Interdire** pour les niveaux d'accès suivants :
  - Cliquez sur **Configuration** dans la sous-section **Modifier les droits de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration des fonctions de Kaspersky Security for Windows Server.
  - Cliquez sur **Configuration** dans la sous-section **Modifier les droits d'utilisateurs pour**

**l'administration de Service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration de l'application à l'aide du Service Kaspersky Security.

La fenêtre de groupe **Autorisations pour Kaspersky Security** s'ouvre.

4. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste **Groupes ou noms d'utilisateurs** l'utilisateur ou le groupe d'utilisateurs pour lequel vous souhaitez modifier les autorisations.
5. Dans la section **Autorisation pour <Utilisateur (Groupe)>**, cochez les cases **Autoriser** ou **Interdire** pour les niveaux d'accès suivants :
  - **Contrôle complet** : sélection complète des autorisations d'administration de Kaspersky Security for Windows Server ou du Service Kaspersky Security.
  - **Lire** :
    - Privilèges suivants d'administration de Kaspersky Security for Windows Server : **Récupérer les statistiques, Lire les paramètres, Lire les journaux et Lire les privilèges.**
    - Privilèges suivants d'administration du Service Kaspersky Security : **Lire les paramètres du service, Solliciter l'état du service auprès du Gestionnaire de contrôle des services, Solliciter le statut auprès du service, Lire la liste des services dépendants, Lire les privilèges.**
  - **Modifier** :
    - Toutes les autorisations d'administration de Kaspersky Security for Windows Server, à l'exception de **Modifier les privilèges.**
    - Privilèges suivants d'administration du Service Kaspersky Security : **Modifier les paramètres du service, Lire les privilèges.**
  - **Privilèges spéciaux** : privilèges suivants d'administration du Service Kaspersky Security : **Lancer le service, Arrêter le service, Suspension/reprise du service, Lire les privilèges, Requêtes de l'utilisateur au service.**
6. Si vous souhaitez réaliser une configuration étendue des autorisations pour un utilisateur ou un groupe d'utilisateurs (**Autorisations spéciales**), cliquez sur le bouton **Avancé**.
  - a. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Security for Windows Server** qui s'ouvre, sélectionnez l'utilisateur ou le groupe souhaité.
  - b. Cliquez sur le bouton **Modifier**.
  - c. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).
  - d. Cochez les cases en regard des fonctions pour lesquelles vous souhaitez octroyer ou non un accès à un utilisateur ou un groupe d'utilisateurs sélectionnés.
  - e. Cliquez sur le bouton **OK**.
  - f. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Security for Windows Server**, cliquez sur **OK**.
7. Dans la fenêtre de groupe **Autorisations pour Kaspersky Security**, cliquez sur le bouton **Appliquer**.

Les autorisations d'administration de Kaspersky Security for Windows Server ou du Service Kaspersky Security configurées sont enregistrées.

## Accès protégé par mot de passe aux fonctions de Kaspersky Security for Windows Server

Vous pouvez limiter l'accès à l'administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)). Vous pouvez renforcer la protection grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Security for Windows Server. La protection par mot de passe constitue une manière supplémentaire de limiter l'accès à l'administration de la Console de l'application et à l'exécution de commandes via la ligne de commande. Quand la protection par mot de passe est appliquée, Kaspersky Security for Windows Server impose à tous les utilisateurs de saisir le mot de passe pour lancer la Console de l'application ou exécuter des commandes via la ligne de commande.

► *Pour protéger l'accès aux fonctions de Kaspersky Security for Windows Server :*

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Security** et réalisez l'une des actions suivantes :
  - Dans le panneau de détails du nœud, suivez le lien **Propriétés de l'application**.
  - Dans le menu contextuel du nœud, sélectionnez l'option **Propriétés**.

La fenêtre **Paramètres de l'application** s'ouvre.

2. Sous l'onglet **Sécurité et fiabilité** des **paramètres de protection par mot de passe**, cochez la case **Utiliser la protection par mot de passe**.

Les champs **Mot de passe** et **Confirmer mot de passe** deviennent actifs.

3. Saisissez dans le champ **Mot de passe** le mot de passe que vous voulez utiliser pour protéger l'accès aux fonctions de Kaspersky Security for Windows Server.
4. Dans le champ **Confirmer mot de passe**, saisissez à nouveau le mot de passe.
5. Cliquez sur le bouton **OK**.

**Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pouvez plus contrôler l'application. Il devient également impossible de désinstaller l'application depuis le serveur protégé.**

Il est possible de réinitialiser le mot de passe à tout moment. Pour ce faire, décochez la case **Utiliser la protection par mot de passe** et enregistrez les modifications. La protection par mot de passe est désactivée et la somme de contrôle de l'ancien mot de passe est supprimée. Répétez le processus de saisie du mot de passe avec un nouveau mot de passe.

## Configuration des autorisations d'accès dans Kaspersky Security Center

Vous pouvez configurer les autorisations d'accès pour l'administration de l'application et du service Kaspersky Security dans Kaspersky Security Center pour un groupe de serveurs ou un serveur individuel.

► *Pour configurer les autorisations d'accès à l'application et au Service Kaspersky Security, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de

Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Ouvrez la section **Complémentaire** et réalisez les opérations suivantes :
  - Si vous souhaitez configurer les autorisations d'accès pour l'administration de Kaspersky Security for Windows Server pour un utilisateur ou un groupe d'utilisateurs, cliquez sur le bouton **Configuration** dans la section **Autorisations d'accès de l'utilisateur pour l'administration de l'application**.
  - Si vous souhaitez configurer les autorisations d'accès pour l'administration du Service Kaspersky Security pour un utilisateur ou un groupe d'utilisateurs, cliquez sur le bouton **Configuration** dans la section **Autorisations d'accès de l'utilisateur pour l'administration du service Security**.
5. Dans la fenêtre qui s'ouvre, configurez les autorisations d'accès (cf. section "Gestion des autorisations d'accès pour les fonctions de Kaspersky Security for Windows Server" à la page [239](#)) en fonction de vos besoins.

Les paramètres définis seront enregistrés.

# Protection des fichiers en temps réel

Cette section contient des informations sur la tâche Protection des fichiers en temps réel et les instructions sur la configuration de cette tâche.

## Contenu du chapitre

A propos de la tâche Protection des fichiers en temps réel .....	<a href="#">248</a>
A propos de la zone de protection de la tâche et des paramètres de sécurité .....	<a href="#">249</a>
A propos de la zone de protection virtuelle .....	<a href="#">250</a>
Zones de protection prédéfinies .....	<a href="#">250</a>
Niveaux de sécurité prédéfinis.....	<a href="#">251</a>
Extensions de fichiers analysés par défaut dans la tâche Protection des fichiers en temps réel .....	<a href="#">253</a>
Paramètres par défaut de la tâche Protection des fichiers en temps réel.....	<a href="#">255</a>
Administration de la tâche de protection des fichiers en temps réel via le plug-in d'administration.....	<a href="#">256</a>
Administration de la tâche de protection des fichiers en temps réel via la Console de l'application.....	<a href="#">271</a>

## A propos de la tâche Protection des fichiers en temps réel

Au cours de l'exécution de la tâche Protection des fichiers en temps réel, Kaspersky Security for Windows Server analyse les objets du serveur protégé suivants lorsqu'ils sont sollicités :

- Les fichiers ;
- Flux alternatifs des systèmes de fichiers (flux NTFS).
- Les enregistrements de démarrage principaux et les secteurs d'amorçage des disques durs locaux ou des périphériques externes.
- Fichiers conteneurs Windows Server 2016 et Windows Server 2019.

Lorsqu'un programme quelconque enregistre un fichier sur le serveur ou tente de le lire, Kaspersky Security for Windows Server intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace, il exécute les actions que vous avez définies dans les paramètres de la tâche ou par défaut : il tente de désinfecter le fichier, le place en quarantaine ou il le supprime. Avant la désinfection ou la suppression, Kaspersky Security for Windows Server enregistre une copie chiffrée du fichier source dans le dossier Sauvegarde. Kaspersky Security for Windows Server restaure le fichier dans le dossier original s'il est sain ou si sa désinfection a réussi.

Kaspersky Security for Windows Server intercepte ses opérations sur les fichiers exécutées dans les conteneurs Windows Server 2016 et Windows Server 2019.

Un *conteneur* est un environnement isolé qui permet aux applications de s'exécuter sans interaction directe avec le système d'exploitation. Si le conteneur se trouve dans la zone de protection de la tâche, Kaspersky Security for Windows Server analyse les fichiers du conteneur lorsqu'ils sont sollicités par les utilisateurs à la recherche de menaces informatiques. En cas de détection d'une menace, l'application tente de désinfecter le conteneur. Si la tentative réussit, le conteneur continue à fonctionner. Si la désinfection échoue, il est arrêté.

Kaspersky Security for Windows Server détecte également les applications malveillantes pour les processus

exécutés dans le sous-système Windows pour Linux®. Pour ces processus, la tâche Protection des fichiers en temps réel applique l'action définie par la configuration actuelle.

## A propos de la zone de protection de la tâche et des paramètres de sécurité

Par défaut, la tâche Protection des fichiers en temps réel protège tous les objets du système de fichiers du serveur. Si la sécurité n'exige pas de protéger tous les objets du système de fichiers ou vous voulez exclure expressément certains objets de la zone d'action de la tâche de protection en temps réel, vous pouvez limiter la zone de protection.

Dans la console de l'application, la zone de protection se présente sous la forme d'une arborescence ou d'une liste ressources de fichiers du serveur que Kaspersky Security for Windows Server peut contrôler. Par défaut les ressources de fichier réseau du serveur protégé s'affichent sous la forme d'une liste.

Seul l'affichage sous forme de liste est disponible dans le plug-in d'administration.

► *Pour activer l'affichage des ressources de fichier réseau sous la forme d'une arborescence dans la Console de l'application,*

dans la liste déroulante du coin supérieur gauche de la fenêtre de configuration de la **Configuration de la zone de protection**, choisissez l'option **Afficher sous forme d'arborescence**.

Les éléments ou les entrées sont présentés dans une liste ou dans une arborescence des ressources de fichiers du serveur de la manière suivante :

- Nœud inclus dans la zone de protection.
- Le nœud est exclu de la zone de protection.
- Au moins un des nœuds enfants intégrés de nœud est exclu de la zone de protection ou les paramètres de sécurité de ces nœuds enfant diffèrent des paramètres de sécurité d'un nœud parent (uniquement pour un mode d'affichage en arborescence)

L'icône  s'affiche si tous les nœuds enfants ont été sélectionnés, mais pas le nœud parent. Dans ce cas, les modifications du contenu des fichiers et dossiers du nœud parent ne sont pas automatiquement prises en compte lors de la constitution de la zone de protection du nœud enfant sélectionné.

La console de l'application permet également d'ajouter des disques virtuels (cf. section "Création d'une zone de protection virtuelle" à la page [279](#)) à la zone de protection. Le nom des entrées virtuelles apparaît en bleu.

### Paramètres de sécurité

Les paramètres de sécurité de la tâche peuvent être configurés globalement pour l'ensemble des nœuds ou des éléments repris dans la zone de protection ou individuellement pour chaque nœud ou élément dans l'arborescence

ou la liste des ressources de fichier du serveur.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Vous pouvez configurer les paramètres de la zone de protection sélectionnée de l'une des manières suivantes :

- Sélection d'un des trois niveaux de sécurité prédéfinis (à la page [251](#)).
- Configuration manuelle des paramètres de sécurité (cf. section "Configuration manuelle des paramètres de sécurité" à la page [264](#)) pour les entrées ou les éléments sélectionnés dans l'arborescence ou la liste des ressources de fichier de l'ordinateur (le niveau de sécurité devient **Personnalisé**).

Vous pouvez enregistrer un ensemble de paramètres pour un nœud ou un élément dans un modèle afin de pouvoir l'appliquer à d'autres nœuds.

## A propos de la zone de protection virtuelle

Kaspersky Security for Windows Server peut analyser non seulement les fichiers et les dossiers 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 du cluster qui sont créés dynamiquement sur le serveur par diverses applications et services.

Si vous avez inclus tous les objets du serveur dans la zone de protection, ces entrées dynamiques seront automatiquement reprises dans la zone de protection. Toutefois, si vous souhaitez attribuer des valeurs particulières aux paramètres de sécurité de ces entrées dynamiques ou si vous avez sélectionné pour la protection en temps réel non pas tout le serveur, mais uniquement quelques secteurs, pour pouvoir inclure les disques, les fichiers ou les dossiers dans la zone de protection, vous devrez d'abord les créer dans la console de l'application ; c'est ce que l'on appelle la spécification d'une zone de protection virtuelle. Les disques, les fichiers ou les dossiers que vous créez existent uniquement dans la console de l'application et non pas dans la structure du système de fichiers du serveur protégé.

Si au moment de composer la zone de protection, vous sélectionnez tous les fichiers ou les répertoires inclus sans choisir le répertoire parent, les répertoires ou les fichiers dynamiques qui s'y trouvent ne seront pas repris automatiquement dans la zone de protection. Vous devez créer des "copies virtuelles" dans la console de l'application et les ajouter à la zone de protection.

## Zones de protection prédéfinies

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Security for Windows Server couvre les zones de protection définies suivantes :

- **Disques durs locaux.** Kaspersky Security for Windows Server protège les fichiers sur les disques durs du serveur.
- **Disques amovibles.** Kaspersky Security for Windows Server protège les fichiers sur les périphériques externes tels que les disques compacts ou amovibles. Vous pouvez inclure ou exclure de la zone de protection tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Réseau.** Kaspersky Security for Windows Server protège les fichiers qui sont enregistrés dans les dossiers



réseau ou qui y sont lus par les applications exécutées sur le serveur. Kaspersky Security for Windows Server ne protège pas les fichiers dans les répertoires réseau lorsqu'ils sont sollicités par des applications depuis d'autres ordinateurs.

- **Disques virtuels.** Vous pouvez inclure dans la zone 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'un cluster

Par défaut, vous pouvez afficher et configurer des zones de protection prédéfinies dans la liste de zones ; vous pouvez également ajouter des zones prédéfinies à la liste au moment de sa création dans les paramètres de la zone de protection.

La zone de protection inclut par défaut tous les secteurs prédéfinis, à l'exception des disques virtuels.

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

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

## Niveaux de sécurité prédéfinis

Pour les entrées sélectionnées dans l'arborescence ou la liste des ressources de fichiers de l'ordinateur, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

### Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si des mesures de sécurité du serveur complémentaires ont été adoptées dans votre réseau, telles que des pare-feu ou des stratégies de sécurité, en plus de Kaspersky Security for Windows Server.

### Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

### Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité informatique élevé.

Tableau 41. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Options	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
<b>Protection des objets</b>	Selon l'extension	En fonction du format	En fonction du format
<b>Protection uniquement des nouveaux fichiers et des fichiers modifiés</b>	Activée	Activée	Désactivée
<b>Actions à exécuter sur les objets infectés et autres</b>	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible
<b>Actions à exécuter sur les objets probablement infectés</b>	Interdire l'accès et placer en quarantaine	Interdire l'accès et exécuter l'action recommandée	Interdire l'accès et placer en quarantaine
<b>Exclure les fichiers</b>	non	non	non
<b>Ne pas détecter</b>	non	non	non
<b>Arrêter si l'analyse dure plus de (s.)</b>	60 s	60 s	60 s
<b>Ne pas analyser les objets composés de plus de (Mo)</b>	8 Mo	8 Mo	Non configuré
<b>Analyser les flux NTFS alternatifs</b>	Oui	Oui	Oui
<b>Analyser les secteurs d'amorçage et la partition MBR</b>	Oui	Oui	Oui
<b>Protection des objets composés</b>	<ul style="list-style-type: none"> <li>Objets compactés*</li> </ul> *Uniquement les objets nouveaux et modifiés	<ul style="list-style-type: none"> <li>Archives SFX*</li> <li>Objets compactés*</li> <li>Objets OLE intégrés*</li> </ul> *Uniquement les objets nouveaux et modifiés	<ul style="list-style-type: none"> <li>Archives SFX*</li> <li>Objets compactés*</li> <li>Objets OLE intégrés*</li> </ul> *Tous les objets
<b>Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré</b>	non	non	Oui

Les paramètres **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift** et **Utiliser l'analyse heuristique** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si, après avoir choisi un des niveaux de sécurité prédéfinis, vous modifiez les paramètres de sécurité **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique**, le niveau de sécurité que vous aviez choisi ne change pas.

## Extensions de fichiers analysés par défaut dans la tâche Protection des fichiers en temps réel

Kaspersky Security for Windows Server analyse par défaut les fichiers possédant les extensions suivantes :

- 386
- *acm*
- *ade, adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*
- *chm*
- *cla, clas\**
- *cmd*
- *com*
- *cpl*
- *crt*
- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*
- *efi*
- *emf*
- *eml*
- *exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm, html\**
- *htt*
- *ico*

- *inf*
- *ini*
- *ins*
- *isp*
- *jpg, jpe*
- *js, jse*
- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*
- *msp*
- *mst*
- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*
- *pht*
- *phtm\**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*
- *shb*

- *shs*
- *sht*
- *shtm\**
- *swf*
- *sys*
- *the*
- *them\**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*
- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

## Paramètres par défaut de la tâche Protection des fichiers en temps réel

Par défaut, la tâche Protection des fichiers en temps réel utilise les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 42. Paramètres par défaut de la tâche Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
<b>Zone de protection</b>	L'ensemble de l'ordinateur, à l'exception des disques virtuels.	Vous pouvez limiter la zone de protection.
<b>Mode de protection d'objets</b>	<b>A l'accès et à la modification</b>	Vous pouvez sélectionner le mode de protection, c'est-à-dire définir le type d'accès auquel Kaspersky Security for Windows Server va analyser l'objet.
<b>Analyse heuristique</b>	Le niveau de sécurité <b>Moyenne</b> est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
<b>Appliquer la zone de confiance</b>	Appliquée.	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.
<b>Utiliser KSN pour la protection</b>	Appliquée.	Vous pouvez améliorer l'efficacité de la protection du serveur en utilisant l'infrastructure de services cloud du Kaspersky Security Network (disponible si la Déclaration du KSN a été acceptée).
Planification du lancement de la tâche	Au lancement de l'application.	Vous pouvez configurer le lancement de la tâche planifiée.
<b>Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante</b>	Pas appliqué.	Vous pouvez ajouter les ordinateurs qui manifestent une activité malveillante à la liste des ordinateurs bloqués.

# Administration de la tâche de protection des fichiers en temps réel via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des serveurs du réseau.

## Dans cette section

Navigation .....	<a href="#">257</a>
Configuration de la tâche Protection des fichiers en temps réel .....	<a href="#">258</a>
Création et configuration de la zone de protection de la tâche .....	<a href="#">263</a>
Configuration manuelle des paramètres de sécurité .....	<a href="#">264</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres de la stratégie pour la tâche Protection des fichiers en temps réel.....	<a href="#">257</a>
Accès aux propriétés de la tâche Protection des fichiers en temps réel .....	<a href="#">258</a>

## Accès aux paramètres de la stratégie pour la tâche Protection des fichiers en temps réel

► *Pour accéder aux paramètres de la tâche Protection des fichiers en temps réel via une stratégie de Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel du serveur**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Protection des fichiers en temps réel**.

La fenêtre **Protection des fichiers en temps réel** s'ouvre.



Si le serveur est administré par une stratégie active de Kaspersky Security Center et que cette stratégie interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés via la Console de l'application.

## Accès aux propriétés de la tâche Protection des fichiers en temps réel

► Pour ouvrir la fenêtre de configuration de la tâche Protection des fichiers en temps réel pour un seul serveur du réseau, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <nom du serveur>** à l'aide d'une des méthodes suivantes :
  - Double-clic sur le nom du serveur protégé.
  - Sélectionnez l'option **Propriétés** dans le menu contextuel du serveur protégé.

La fenêtre **Propriétés : <nom du serveur>** s'ouvre.

5. Dans la section **Tâches**, sélectionnez la tâche **Protection des fichiers en temps réel**.
6. Cliquez sur le bouton **Propriétés**.

La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.

## Configuration de la tâche Protection des fichiers en temps réel

► Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel" à la page [257](#)).
2. Configurez les paramètres de la tâche suivants :
  - Sous l'onglet **Général** :
    - **Mode de protection d'objets** (cf. section "**Sélection du mode de protection**" à la page [259](#))
    - **Analyse heuristique**
    - **Intégration aux autres composants** (cf. section "**Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application**" à la page [260](#))
  - Sous l'onglet **Administration des tâches** :
    - Paramètres de lancement de la tâche planifiée (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [138](#)).
3. Sélectionnez l'onglet **Zone de protection**, puis réalisez les opérations suivantes :

- Cliquez sur le bouton **Ajouter** ou **Modifier** pour modifier la zone de protection (cf. section "Création d'une zone de protection" à la page [276](#)).
    - Dans la fenêtre qui s'ouvre, sélectionnez les éléments que vous souhaitez inclure dans la zone de protection de la tâche :
      - **Zone prédéfinie**
      - **Disque, dossier ou objet réseau**
      - **Fichier**
    - Sélectionnez un des niveaux de sécurité prédéfinis (cf. page [251](#)) ou configurez manuellement les paramètres de protection (cf. section "Configuration manuelle des paramètres de sécurité" à la page [264](#)).
4. Cliquez sur le bouton **OK** dans la fenêtre **Protection des fichiers en temps réel**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Dans cette section

Sélection du mode de protection .....	<a href="#">259</a>
Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application .....	<a href="#">260</a>
Configuration des paramètres de la planification du lancement de la tâche .....	<a href="#">261</a>

## Sélection du mode de protection

La tâche Protection des fichiers en temps réel permet de sélectionner le mode de protection. La section **Mode de protection d'objets** permet de définir le type d'accès aux objets déclenchant une analyse par Kaspersky Security for Windows Server.

Le paramètre **Mode de protection d'objets** possède une valeur unique pour toute la zone de protection reprise dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les entrées particulières de la zone de protection.

### ► Pour sélectionner le mode de protection :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel" à la page [257](#)).
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection que vous souhaitez définir :
  - **Mode intelligent**

Kaspersky Security for Windows Server sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si un processus contacte et modifie plusieurs fois un objet pendant son exécution, Kaspersky Security for Windows Server analyse à nouveau cet objet uniquement après la dernière sauvegarde effectuée par ce processus.
  - **A l'accès et à la modification**

Kaspersky Security for Windows Server analyse l'objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié.

Cette option est sélectionnée par défaut.

- **A l'accès**

Kaspersky Security for Windows Server analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

- **A l'exécution**

Kaspersky Security for Windows Server analyse le fichier uniquement en cas d'ouverture pour exécution.

3. Cliquez sur le bouton **OK**.

Le mode de protection des objets sélectionné sera adopté.

## Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

► *Pour configurer l'analyse heuristique et l'intégration aux autres composants, procédez comme suit :*

1. Ouvrez la fenêtre **Protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel" à la page [257](#)).

2. Sous l'onglet **Général**, cochez ou décochez la case **Utiliser l'analyse heuristique**.

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

3. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

Il existe trois niveaux de détail pour l'analyse

- **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.

- **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

Il s'agit du niveau par défaut.

- **Minutieuse**. L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le

nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

4. Configurez les paramètres suivants dans la section **Intégration aux autres composants** :

- Cochez ou décochez la case **Appliquer la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

- Cochez ou décochez la case **Utiliser KSN pour la protection**.

Cette case active ou désactive l'utilisation des services KSN.

Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs.

Si la case est décochée, la tâche n'utilise pas les services du KSN.

Cette case est cochée par défaut.

La case **Envoyer des données sur les fichiers analysés** doit être cochée dans les paramètres de la tâche **Utilisation du KSN**.

- Cochez ou décochez la case **Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante**.

5. Cliquez sur le bouton **OK**.

Les paramètres configurés de la tâche seront appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

## Configuration des paramètres de la planification du lancement de la tâche

La console de l'application permet de planifier le lancement des tâches locales du système et définies par l'utilisateur. Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement de la tâche de groupe, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.
2. Sélectionnez le groupe auquel appartient le serveur protégé.
3. Dans le panneau de détails, choisissez l'onglet **Tâches**.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

- Double-cliquez sur le nom de la tâche.
  - Ouvrez le menu contextuel du nom de la tâche et sélectionnez l'option Propriétés.
5. Sélectionnez la section **Planification**.
  6. Dans le groupe **Paramètres de planification**, cochez la case **Exécuté selon la programmation**.

Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée est interdite par une stratégie de Kaspersky Security Center.

7. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
  - a. Choisissez une des options suivantes dans la liste **Fréquence** :
    - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
    - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
    - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;
    - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security for Windows Server.
    - **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.
  - b. Indiquez, dans le champ **Démarrer à**, l'heure du premier lancement de la tâche.
  - c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

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, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est interdit par les paramètres d'une stratégie active de Kaspersky Security Center (cf. section "Configuration de la planification de l'exécution programmée des tâches locales du système" à la page. [104](#)).

8. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.
  - Dans la section **Paramètres d'arrêt de la tâche** :
    - a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la tâche.
    - b. Cochez la case **Pause à partir de**, puis saisissez les heures de début et de fin pour spécifier un intervalle de temps de moins de 24 heures pendant lequel l'exécution de la tâche sera suspendue.
  - Dans la section **Paramètres avancés** :

- a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.
  - b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.
  - c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.
9. Cliquez sur le bouton **OK**.
  10. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

Si vous souhaitez configurer les paramètres de l'application pour une tâche unique à l'aide de Kaspersky Security Center, suivez les étapes décrites à la section Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center (à la page [127](#)).

## Création et configuration de la zone de protection de la tâche

► Pour créer et configurer la zone de protection de la tâche via Kaspersky Security Center, procédez comme suit :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel" à la page [257](#)).
2. Ouvrez l'onglet **Zone de protection**.
3. Tous les éléments déjà couverts par la protection sont repris dans le tableau **Zone de protection**.
4. Cliquez sur le bouton **Ajouter** pour ajouter un nouvel élément à la liste.

La fenêtre **Ajouter des objets à la zone de protection** s'ouvre.

5. Sélectionnez un type d'objet pour l'ajouter à une zone de protection :
  - **Zone prédéfinie**, si vous voulez insérer dans la zone de protection une des zones prédéfinies sur le serveur protégé. Puis, dans la liste déroulante, choisissez la zone de protection nécessaire.
  - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone de protection un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone de protection requise en cliquant sur le bouton **Parcourir**.
  - **Fichier**, si vous voulez insérer dans la zone de protection uniquement un fichier distinct sur le disque. Puis choisissez la zone de protection requise en cliquant sur le bouton **Parcourir**.

**Vous ne pouvez pas ajouter un objet à la zone de protection s'il est déjà ajouté en tant qu'exclusion de la zone de protection.**

6. Pour exclure certains éléments de la zone de protection, décochez les cases en regard des noms de ces éléments ou réalisez les opérations suivantes :
  - a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.
  - b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.
  - c. Dans la fenêtre **Ajouter une exclusion**, choisissez le type de l'objet que vous voulez ajouter à titre d'exclusion de la zone de protection, de la même manière que l'ajout d'un objet à la zone de protection.

7. Pour modifier la zone de protection ou l'exclusion ajoutée, dans le menu contextuel de la zone de protection que vous voulez modifier, choisissez l'option **Modifier la zone**.
8. Pour masquer l'affichage d'une zone de protection ou d'une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone de protection que vous voulez masquer, choisissez l'option **Supprimer une zone**.

La zone de protection est exclue de la zone d'action de la tâche **Protection des fichiers en temps réel** lors de sa suppression de la liste des ressources de fichier réseau.

9. Cliquez sur le bouton **Enregistrer**.

La fenêtre de configuration de la Zone de protection est fermée. Les nouvelles valeurs des paramètres seront enregistrés.

Vous ne pourrez exécuter la tâche **Protection des fichiers en temps réel** que si au moins une entrée de l'arborescence des ressources de fichiers de l'ordinateur est incluse dans la zone de protection.

## Configuration manuelle des paramètres de sécurité

Par défaut, la tâche **Protection des fichiers en temps réel** applique les mêmes paramètres de sécurité à toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé** (cf. section "Niveaux de sécurité prédéfinis" à la page [251](#)).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers du serveur.

► *Pour configurer manuellement les paramètres de sécurité du nœud sélectionnée :*

1. Ouvrez la fenêtre **Protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche **Protection des fichiers en temps réel**" à la page [257](#)).
2. Sous l'onglet **Zone de protection**, choisissez le nœud dont vous souhaitez configurer les paramètres de sécurité, puis cliquez sur le bouton **Configurer**.

La fenêtre **Paramètres de la protection des fichiers en temps réel** s'ouvre.

3. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Configuration** pour définir la configuration personnalisée.
4. Vous pouvez configurer les paramètres de sécurité personnalisés du nœud sélectionné en fonction de vos exigences.
  - Paramètres généraux (cf. section "Configuration des règles prédéfinies d'une tâche" à la page [265](#))
  - Actions (cf. section "Configuration des actions" à la page [267](#))
  - Optimisation (cf. section "Configuration de l'optimisation" à la page [269](#))
5. Cliquez sur le bouton **OK** dans la fenêtre **Protection des fichiers en temps réel**.

Les paramètres de la nouvelle zone de protection sont enregistrés.



## Dans cette section

Configuration des paramètres de tâche généraux .....	<a href="#">265</a>
Configuration des actions .....	<a href="#">267</a>
Configuration de l'optimisation.....	<a href="#">269</a>

## Configuration des paramètres de tâche généraux

### ► Configuration des paramètres généraux de sécurité de la tâche Protection des fichiers en temps réel

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel" à la page [257](#)).
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Protection des objets**, indiquez les types d'objets que vous souhaitez inclure à la zone de protection :

- **Tous les objets**

Kaspersky Security for Windows Server analyse tous les objets.

- **Objets analysés en fonction du format**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- **Analyser les secteurs d'amorçage et la partition MBR**

Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

Si la case est cochée, Kaspersky Security for Windows Server analyse les secteurs et les zones d'amorce sur les disques durs et les disques amovibles du serveur.

Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**

Analyse des flux complémentaires de fichiers et de dossiers dans les disques du système



de fichiers NTFS.

Si la case est cochée, l'application analyse un objet probablement infecté et tous les flux NTFS associés à cet objet.

Si la case est décochée, l'application analyse uniquement l'objet qui a été détecté et considéré comme probablement infecté.

Cette case est cochée par défaut.

4. Dans la section **Optimisation**, cochez ou décochez la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés**.

La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security for Windows Server a identifiés comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

Si la case est cochée, Kaspersky Security for Windows Server analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

Si la case est décochée, vous pouvez décider si vous souhaitez analyser et protéger uniquement les nouveaux fichiers ou tous les fichiers, quel que soit leur état de modification.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Protection maximale** ou **Recommandé**, la case est décochée.

Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.

5. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :

- **Toutes les/ Les nouvelles archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Toutes les /Les nouvelles archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données d'emails**

Analyse des fichiers des bases de données de messagerie de Microsoft Outlook et

Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers des bases de données de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers des bases de données de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Tous les / Les nouveaux messages de texte brut**

Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers aux formats de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers aux formats de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration des actions

► *Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "**Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel**" à la page [257](#)).
2. Sélectionnez l'onglet **Actions**.

3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

- **Informier uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informier uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Bloquer l'accès.**

Lorsque cette option est sélectionnée, Kaspersky Security for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.

- **Exécuter une action supplémentaire.**

Sélectionnez l'action dans la liste déroulante.

- **Désinfecter.**
- **Désinfecter. Supprimer si la désinfection est impossible.**
- **Supprimer.**
- **Recommandé.**

4. Sélectionnez l'action à exécuter sur les objets probablement infectés :

- **Informier uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informier uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Bloquer l'accès.**

Lorsque cette option est sélectionnée, Kaspersky Security for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.

- **Exécuter une action supplémentaire.**

Sélectionnez l'action dans la liste déroulante.

- **Quarantaine.**
- **Supprimer.**

- **Recommandé.**

5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

Si la case est cochée, vous pouvez indépendamment définir une action principale et secondaire pour chaque type d'objet détecté en cliquant sur le bouton **Configuration** en regard de la case. De plus, Kaspersky Security for Windows Server ne permet pas d'ouvrir ou d'exécuter un objet infecté, quel que soit votre choix.

Si la case est décochée, Kaspersky Security for Windows Server exécute les actions sélectionnées dans les sections **Actions à exécuter sur les objets infectés et autres** et **Actions à exécuter sur les objets probablement infectés** des types d'objets nommés, respectivement.

Cette case est décochée par défaut.

b. Cliquez sur le bouton **Configuration**.

c. Dans la fenêtre qui s'ouvre, choisissez la première action et l'action secondaire (si la première échoue) pour chaque type de l'objet détecté.

d. Cliquez sur le bouton **OK**.

6. Choisissez l'action à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**.

La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.

7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration de l'optimisation

► *Pour configurer l'optimisation de la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel** (cf. section "**Accès aux paramètres de stratégie pour la tâche Protection des fichiers en temps réel**" à la page [257](#)).

2. Sélectionnez l'onglet **Optimisation**.

3. Dans la section **Exclusions** :

- Cochez ou décochez la case **Exclure les fichiers**.

Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse tous les objets.

Cette case est décochée par défaut.

- Cochez ou décochez la case **Ne pas détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus <https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

#### 4. Dans la section **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets composés de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Si la case est cochée, Kaspersky Security for Windows Server ignore pour la recherche de virus les objets composés dont la taille est supérieure à la valeur indiquée.

Si la case est décochée, Kaspersky Security for Windows Server analyse les objets composés sans tenir compte de la taille.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Utiliser la technologie iSwift**

iSwift compare l'identifiant NTFS du fichier, identifiant stocké dans une base de données, avec un identifiant en cours. L'analyse est effectuée uniquement pour les fichiers dont les identifiant ont changé (nouveaux fichiers et fichiers modifiés depuis la dernière analyse des objets système NTFS).

Si la case est cochée, Kaspersky Security for Windows Server analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse des objets système NTFS.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers du système NTFS en ignorant la date de création ou de modification sauf pour les fichiers des dossiers réseau.

Cette case est cochée par défaut.

- **Utiliser la technologie iChecker**

iChecker calcule et enregistre les sommes de contrôle des fichiers analysés. Si un objet est modifié, la somme de contrôle change. L'application compare toutes les sommes de contrôle pendant la tâche d'analyse et analyse uniquement les fichiers nouveaux et modifiés depuis la dernière analyse de fichiers.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers nouveaux et modifiés.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers en ignorant leur date de création ou de modification.

Cette case est cochée par défaut.

## Administration de la tâche de protection des fichiers en temps réel via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un serveur local.

### Dans cette section

Navigation .....	<a href="#">271</a>
Accès aux paramètres de la zone de protection des fichiers en temps réel .....	<a href="#">271</a>
Accès aux paramètres de la tâche Protection des fichiers en temps réel .....	<a href="#">272</a>
Configuration de la tâche Protection des fichiers en temps réel .....	<a href="#">272</a>
Constitution de la zone de protection .....	<a href="#">276</a>
Configuration manuelle des paramètres de sécurité .....	<a href="#">279</a>
Statistiques de la tâche Protection des fichiers en temps réel .....	<a href="#">286</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Accès aux paramètres de la zone de protection des fichiers en temps réel

► *Pour ouvrir la fenêtre des paramètres de la Zone de protection de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.

2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.
3. Dans le panneau de détails, cliquez sur le lien **Configurer la zone de protection**.  
La fenêtre **Configuration de la zone de protection** s'ouvre.

## Accès aux paramètres de la tâche Protection des fichiers en temps réel

► *Pour ouvrir la fenêtre de configuration des paramètres généraux d'une tâche, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.

## Configuration de la tâche Protection des fichiers en temps réel

► *Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "Accès aux paramètres de la tâche Protection des fichiers en temps réel" à la page [272](#)).
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
  - **Mode de protection d'objets** (cf. section "**Sélection du mode de protection**" à la page [273](#))
  - **Analyse heuristique**
  - **Intégration aux autres composants** (cf. section "**Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application**" à la page [274](#))
3. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)).
4. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.  
Les modifications apportées aux paramètres seront enregistrées.
5. Dans le panneau de détails du nœud **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.
6. Exécutez les actions suivantes :
  - Dans l'arborescence ou la liste des ressources de fichier du serveur, sélectionnez les entrées ou les éléments à inclure dans la zone de protection de la tâche.
  - Sélectionnez un des niveaux de sécurité prédéfinis ou configurez les paramètres de protection de l'objet manuellement (cf. Section "Configuration manuelle des paramètres de sécurité" à la page [510](#)).
7. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche définis avant et après leur modification, sont enregistrées dans le journal

d'audit système.

## Dans cette section

Sélection du mode de protection .....	<a href="#">273</a>
Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application .....	<a href="#">274</a>
Configuration des paramètres de la planification du lancement de la tâche .....	<a href="#">275</a>

## Sélection du mode de protection

La tâche Protection des fichiers en temps réel permet de sélectionner le mode de protection. La section **Mode de protection d'objets** permet de définir le type d'accès aux objets déclenchant une analyse par Kaspersky Security for Windows Server.

Le paramètre **Mode de protection d'objets** possède une valeur unique pour toute la zone de protection reprise dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les entrées particulières de la zone de protection.

► *Pour sélectionner le mode de protection des objets, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "Accès aux paramètres de la tâche Protection des fichiers en temps réel" à la page [272](#)).
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection que vous souhaitez définir :

- **Mode intelligent**

Kaspersky Security for Windows Server sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si un processus contacte et modifie plusieurs fois un objet pendant son exécution, Kaspersky Security for Windows Server analyse à nouveau cet objet uniquement après la dernière sauvegarde effectuée par ce processus.

- **A l'accès et à la modification**

Kaspersky Security for Windows Server analyse l'objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié.

Cette option est sélectionnée par défaut.

- **A l'accès**

Kaspersky Security for Windows Server analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

- **A l'exécution**

Kaspersky Security for Windows Server analyse le fichier uniquement en cas d'ouverture pour exécution.

3. Cliquez sur le bouton **OK**.

Le mode de protection des objets sélectionné sera adopté.



## Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

► Pour configurer l'analyse heuristique et l'intégration aux autres composants, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection des fichiers en temps réel**" à la page [272](#)).
2. Sous l'onglet **Général**, cochez ou décochez la case **Utiliser l'analyse heuristique**.

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

3. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

Il existe trois niveaux de détail pour l'analyse

- **Superficielle.** L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
- **Moyenne.** L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.  
Il s'agit du niveau par défaut.
- **Minutieuse.** L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

4. Configurez les paramètres suivants dans la section **Intégration aux autres composants** :

- Cochez ou décochez la case **Appliquer la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

Le lien **Zone de confiance** permet d'accéder aux paramètres de la Zone de confiance.

- Cochez ou décochez la case **Utiliser KSN pour la protection**.

Cette case active ou désactive l'utilisation des services KSN.

Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs.

Si la case est décochée, la tâche n'utilise pas les services du KSN.

Cette case est cochée par défaut.

La case **Envoyer des données sur les fichiers analysés** doit être cochée dans les paramètres de la tâche **Utilisation du KSN**.

- Cochez ou décochez la case **Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante**.

5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront appliqués.

## Configuration des paramètres de la planification du lancement de la tâche

La console de l'application permet de planifier le lancement des tâches locales du système et définies par l'utilisateur. Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement de la tâche, procédez comme suit :*

1. Ouvrez le menu contextuel de la tâche dont vous souhaitez configurer la planification du lancement.
2. Choisissez l'option **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la programmation**.
4. Configurez l'heure en fonction de vos besoins. Pour ce faire, procédez comme suit :

- a. Choisissez une des options suivantes dans la liste **Fréquence** :

- **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
- **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
- **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s) le**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi) ;
- **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Security for Windows Server.
- **A la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.

- b. Indiquez, dans le champ **Démarrer à**, l'heure du premier lancement de la tâche.

- c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

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, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est défini par les paramètres de la stratégie de Kaspersky Security Center.

5. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.
  - Dans la section **Paramètres d'arrêt de la tâche** :
    - a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la tâche.
    - b. Cochez la case **Pause à partir de**, puis saisissez les heures de début et de fin pour spécifier un intervalle de temps de moins de 24 heures pendant lequel l'exécution de la tâche sera suspendue.
  - Dans la section **Paramètres avancés** :
    - a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.
    - b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.
    - c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.
6. Cliquez sur le bouton **OK**.

La configuration des paramètres de lancement de la tâche est enregistrée.

## Constitution de la zone de protection

Cette section contient des informations sur la constitution et l'utilisation de la zone de protection dans la tâche Protection des fichiers en temps réel et sur son utilisation.

### Dans cette section

Constitution de la zone de protection .....	<a href="#">276</a>
Création d'une zone de protection virtuelle .....	<a href="#">279</a>

## Constitution de la zone de protection

La procédure de constitution de la zone de protection dans la tâche Protection des fichiers en temps réel dépend du mode d'affichage des ressources de fichier réseau (cf. section "A propos de la zone de protection et des paramètres de sécurité" à la page [249](#)). Vous pouvez configurer l'affichage des ressources de fichier réseau sous la forme d'une liste (est appliqué par défaut) ou sous la forme d'une arborescence.

Pour appliquer les nouveaux paramètres de la zone de protection à la tâche, il faut relancer la tâche Protection des fichiers en temps réel.

► *Pour créer une zone de protection à l'aide de l'arborescence des ressources de fichier réseau, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. Dans la partie gauche de la fenêtre ouverte déployez l'arborescence des ressources de fichier réseau pour afficher tous les nœuds et les nœuds enfants.
3. Exécutez les actions suivantes :
  - Pour exclure certaines entrées de la zone de protection, décochez les cases à côté des noms de ces entrées.
  - Pour inclure certains nœuds à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :
    - Si vous souhaitez inclure tous les disques d'un même type dans la zone de protection, 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 dans la zone de protection, développez le nœud 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:, développez le nœud **Disques amovibles** et cochez la case en regard du disque **F:**.
    - Si vous souhaitez inclure dans la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case en regard de ce dossier ou de ce fichier.
4. Cliquez sur le bouton **Enregistrer**.

La fenêtre des paramètres de la Zone de protection se ferme. Les paramètres de la tâche définis seront enregistrés.

► *Pour créer une zone de protection à l'aide de la liste des ressources de fichier réseau, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. Pour inclure certains nœuds à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :
  - a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.
  - b. Dans le menu contextuel, sélectionnez l'option **Ajouter une zone de protection**.
  - c. Dans la fenêtre **Ajouter une zone de protection** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter à la zone de protection :
    - **Zone prédéfinie**, si vous voulez insérer dans la zone de protection une des zones prédéfinies sur le serveur protégé. Puis, dans la liste déroulante, choisissez la zone de protection nécessaire.
    - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone de protection un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone requise en cliquant

sur le bouton **Parcourir**.

- **Fichier**, si vous voulez insérer dans la zone de protection uniquement un fichier distinct sur le disque. Puis choisissez la zone requise en cliquant sur le bouton **Parcourir**.

**Vous ne pouvez pas ajouter un objet à la zone de protection s'il est déjà ajouté en tant qu'exclusion de la zone de protection.**

3. Pour exclure certaines entrées de la zone de protection, décochez les cases en regard des noms de ces entrées ou réalisez les opérations suivantes :
  - a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.
  - b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.
  - c. Dans la fenêtre **Ajouter une exclusion**, choisissez le type de l'objet que vous voulez ajouter à titre d'exclusion de la zone de protection, de la même manière que l'ajout d'un objet à la zone de protection.
4. Pour modifier la zone de protection ou l'exclusion ajoutée, dans le menu contextuel de la zone de protection que vous voulez modifier, choisissez l'option **Modifier la zone**.
5. Pour masquer l'affichage d'une zone de protection ou d'une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone de protection nécessaire, choisissez l'option **Supprimer de la liste**.

**La zone de protection est exclue de la zone d'action de la tâche Protection des fichiers en temps réel lors de sa suppression de la liste des ressources de fichier réseau.**

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre des paramètres de la Zone de protection se ferme. Les paramètres de la tâche définis seront enregistrés.

**Vous ne pourrez exécuter la tâche Protection des fichiers en temps réel que si au moins une entrée de l'arborescence des ressources de fichiers de l'ordinateur est incluse dans la zone de protection.**

**Si vous définissez une zone de protection complexe, par exemple en attribuant différentes valeurs aux paramètres de sécurité pour diverses entrées distinctes de l'arborescence des ressources fichiers du serveur, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.**

## Création d'une zone de protection virtuelle

Vous pouvez ajouter à la zone de protection/d'analyse des disques virtuels, des dossiers ou des fichiers distincts, uniquement si la zone de protection/d'analyse s'affiche sous la forme d'une arborescence de ressources de fichier (cf. section "Configuration des paramètres de l'affichage des ressources de fichier réseau" à la page [506](#)).

► Pour ajouter un disque virtuel à la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Ouvrez le menu contextuel du nœud **Disques virtuels**.
4. Sélectionnez l'option **Ajouter un disque virtuel**.
5. Dans la liste des noms disponibles, sélectionnez le nom du disque virtuel en cours de création.
6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone de protection.
7. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.  
Les paramètres de la tâche définis seront enregistrés.

► Pour ajouter un dossier ou un fichier virtuel dans la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Ouvrez le menu contextuel du disque virtuel auquel vous souhaitez ajouter un dossier ou un fichier, puis choisissez une des options suivantes :
  - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone de protection.
  - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone de protection.
4. Dans le champ, saisissez le nom du dossier ou du fichier.
5. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone de protection.
6. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

## Configuration manuelle des paramètres de sécurité

Par défaut, les tâches de protection en temps réel appliquent les mêmes paramètres de sécurité à toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé** (cf. section "Niveaux de sécurité prédéfinis" à la page [251](#)).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de

protection ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers du serveur.

Lorsque vous utilisez l'arborescence des ressources du fichier serveur, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

► *Pour configurer manuellement les paramètres de sécurité :*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le nœud dont vous souhaitez configurer les paramètres de sécurité.

Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité (cf. section "A propos des modèles de paramètres de sécurité" à la page [164](#)) à un nœud ou un élément sélectionné dans la zone de protection.

3. Configurez les paramètres de sécurité requis pour le nœud ou l'élément sélectionné en fonction de vos exigences :
  - **Général** (cf. section "**Configuration des règles prédéfinies d'une tâche**" à la page [280](#))
  - **Actions** (cf. section "**Configuration des actions**" à la page [283](#))
  - **Optimisation** (cf. section "**Configuration de l'optimisation**" à la page [285](#))
4. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.  
Les paramètres de la nouvelle zone de protection sont enregistrés.

## Dans cette section

Configuration des paramètres de tâche généraux .....	<a href="#">280</a>
Configuration des actions .....	<a href="#">283</a>
Configuration de l'optimisation.....	<a href="#">285</a>

## Configuration des paramètres de tâche généraux

► *Configuration des paramètres généraux de sécurité de la tâche Protection des fichiers en temps réel*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Protection des objets**, indiquez les objets que vous souhaitez inclure dans la zone de protection :

- **Tous les objets**

Kaspersky Security for Windows Server analyse tous les objets.

- **Objets analysés en fonction du format**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- **Analyser les secteurs d'amorçage et la partition MBR**

Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

Si la case est cochée, Kaspersky Security for Windows Server analyse les secteurs et les zones d'amorce sur les disques durs et les disques amovibles du serveur.

Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**

Analyse des flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

Si la case est cochée, l'application analyse un objet probablement infecté et tous les flux NTFS associés à cet objet.

Si la case est décochée, l'application analyse uniquement l'objet qui a été détecté et considéré comme probablement infecté.

Cette case est cochée par défaut.

4. Dans la section **Optimisation**, cochez ou décochez la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés**.

La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security for Windows Server a identifiés comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

Si la case est cochée, Kaspersky Security for Windows Server analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

Si la case est décochée, vous pouvez décider si vous souhaitez analyser et protéger uniquement les nouveaux fichiers ou tous les fichiers, quel que soit leur état de modification.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Protection maximale** ou **Recommandé**, la case est décochée.



Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.

5. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :

- **Toutes les/ Les nouvelles archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Toutes les /Les nouvelles archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données d'emails**

Analyse des fichiers des bases de données de messagerie de Microsoft Outlook et Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers des bases de données de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers des bases de données de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Tous les / Les nouveaux messages de texte brut**

Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers aux formats de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers aux

formats de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration des actions

► *Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).
2. Sélectionnez l'onglet **Actions**.
3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Bloquer l'accès.**

Lorsque cette option est sélectionnée, Kaspersky Security for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.

- **Exécuter une action supplémentaire.**

Sélectionnez l'action dans la liste déroulante.

- **Désinfecter.**
- **Désinfecter. Supprimer si la désinfection est impossible.**
- **Supprimer.**

- **Recommandé.**
4. Sélectionnez l'action à exécuter sur les objets probablement infectés :
- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.
  - **Bloquer l'accès.**

Lorsque cette option est sélectionnée, Kaspersky Security for Windows Server bloque l'accès à l'objet détecté ou probablement infecté. Vous pouvez sélectionner une action supplémentaire sur les objets bloqués dans la liste déroulante.
  - **Exécuter une action supplémentaire.**

Sélectionnez l'action dans la liste déroulante.

    - **Quarantaine.**
    - **Supprimer.**
    - **Recommandé.**
5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
- a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

Si la case est cochée, vous pouvez indépendamment définir une action principale et secondaire pour chaque type d'objet détecté en cliquant sur le bouton **Configuration** en regard de la case. De plus, Kaspersky Security for Windows Server ne permet pas d'ouvrir ou d'exécuter un objet infecté, quel que soit votre choix.

Si la case est décochée, Kaspersky Security for Windows Server exécute les actions sélectionnées dans les sections **Actions à exécuter sur les objets infectés et autres** et **Actions à exécuter sur les objets probablement infectés** des types d'objets nommés, respectivement.

Cette case est décochée par défaut.
  - b. Cliquez sur le bouton **Configuration**.
  - c. Dans la fenêtre qui s'ouvre, choisissez la première action et l'action secondaire (si la première échoue) pour chaque type de l'objet détecté.
  - d. Cliquez sur le bouton **OK**.
6. Choisissez l'action à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**.
- La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.

7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration de l'optimisation

► *Pour configurer l'optimisation de la tâche Protection des fichiers en temps réel :*

1. Ouvrez la fenêtre **Configuration de la zone de protection** (cf. section "Accès aux paramètres de la zone de protection des fichiers en temps réel" à la page [271](#)).

2. Sélectionnez l'onglet **Optimisation**.

3. Dans la section **Exclusions** :

- Cochez ou décochez la case **Exclure les fichiers**.

Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse tous les objets.

Cette case est décochée par défaut.

- Cochez ou décochez la case **Ne pas détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus <https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

4. Dans la section **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets composés de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Si la case est cochée, Kaspersky Security for Windows Server ignore pour la recherche de virus les objets composés dont la taille est supérieure à la valeur indiquée.

Si la case est décochée, Kaspersky Security for Windows Server analyse les objets composés sans tenir compte de la taille.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Utiliser la technologie iSwift**

iSwift compare l'identifiant NTFS du fichier, identifiant stocké dans une base de données, avec un identifiant en cours. L'analyse est effectuée uniquement pour les fichiers dont les identifiant ont changé (nouveaux fichiers et fichiers modifiés depuis la dernière analyse des objets système NTFS).

Si la case est cochée, Kaspersky Security for Windows Server analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse des objets système NTFS.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers du système NTFS en ignorant la date de création ou de modification sauf pour les fichiers des dossiers réseau.

Cette case est cochée par défaut.

- **Utiliser la technologie iChecker**

iChecker calcule et enregistre les sommes de contrôle des fichiers analysés. Si un objet est modifié, la somme de contrôle change. L'application compare toutes les sommes de contrôle pendant la tâche d'analyse et analyse uniquement les fichiers nouveaux et modifiés depuis la dernière analyse de fichiers.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers nouveaux et modifiés.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers en ignorant leur date de création ou de modification.

Cette case est cochée par défaut.

## Statistiques de la tâche Protection des fichiers en temps réel

Pendant l'exécution de la tâche Protection des fichiers en temps réel, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security for Windows Server depuis le lancement de cette tâche jusqu'à maintenant.

► *Pour consulter les statistiques de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.

2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Vous pouvez consulter les informations sur les objets que Kaspersky Security for Windows Server a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous) :

Tableau 43. Statistiques de la tâche Protection des fichiers en temps réel

Champ	Description
<b>Détecté</b>	Nombre d'objets détectés par Kaspersky Security for Windows Server. Par exemple, si Kaspersky Security for Windows Server a découvert une application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
<b>Objets infectés et autres détectés</b>	Nombre d'objets que Kaspersky Security for Windows Server a détectés et classés comme infectés ou nombre de fichiers logiciels légitimes détectés et que des intrus peuvent utiliser pour endommager votre ordinateur ou vos données personnelles.
<b>Objets probablement infectés détectés</b>	Nombre d'objets découverts par Kaspersky Security for Windows Server et considérés comme probablement infectés.
<b>Objets non désinfectés</b>	Nombre d'objets que Kaspersky Security for Windows Server n'a pas pu désinfecter pour les raisons suivantes : <ul style="list-style-type: none"> <li>• Le type d'objet détecté ne peut être désinfecté.</li> <li>• une erreur s'est produite lors de la désinfection.</li> </ul>
<b>Objets non placés en quarantaine</b>	Nombre d'objets que Kaspersky Security for Windows Server a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.
<b>Objets non supprimés</b>	Nombre d'objets que Kaspersky Security for Windows Server a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
<b>Objets non analysés</b>	Nombre d'objets de la zone de protection que Kaspersky Security for Windows Server n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
<b>Objets non sauvegardés</b>	Nombre d'objets dont Kaspersky Security for Windows Server a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
<b>Erreurs de traitement</b>	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
<b>Objets désinfectés</b>	Nombre d'objets désinfectés par Kaspersky Security for Windows Server.
<b>Objets placés en quarantaine</b>	Nombre d'objets placés en quarantaine par Kaspersky Security for Windows Server.
<b>Objets sauvegardés</b>	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security for Windows Server.
<b>Objets supprimés</b>	Nombre d'objets supprimés par Kaspersky Security for Windows Server.

Champ	Description
<b>Objets protégés par mot de passe</b>	Nombre d'objets (archives, par exemple) que Kaspersky Security for Windows Server a ignorés en raison d'une protection par mot de passe.
<b>Objets endommagés</b>	Nombre d'objets que Kaspersky Security for Windows Server a ignorés à cause de leur format endommagé.
<b>Objets traités</b>	Nombre d'objets traités par Kaspersky Security for Windows Server.

Vous pouvez également consulter les statistiques de la tâche Protection des fichiers en temps réel dans le journal d'exécution de la tâche via le lien **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du volet résultats.

Si la valeur dans le champ **Total des événements** de la fenêtre du journal d'exécution de la tâche Protection en temps réel est supérieure à 0, il est recommandé de traiter manuellement les événements du journal d'exécution de la tâche sous l'onglet **Événements**.

# Monitoring des scripts

Cette section contient des informations sur la tâche Monitoring des scripts et les instructions sur la configuration de cette tâche.

## Contenu du chapitre

A propos de la tâche Monitoring des scripts .....	<a href="#">289</a>
Paramètres par défaut de la tâche Monitoring des scripts .....	<a href="#">290</a>
Configuration des paramètres de la tâche Monitoring des scripts via le Plug-in d'administration .....	<a href="#">290</a>
Configuration des paramètres de la tâche Monitoring des scripts via la Console de l'application .....	<a href="#">292</a>
Statistiques de la tâche Monitoring des scripts .....	<a href="#">293</a>

## A propos de la tâche Monitoring des scripts

Au cours de l'exécution de la tâche Monitoring des scripts, Kaspersky Security for Windows Server contrôle l'exécution des scripts créés à l'aide des technologies Microsoft Windows Script Technologies (ou Active Scripting), par exemple les scripts VBScript ou JScript®. L'application peut également traiter les scripts PowerShell™ et les scripts exécutés dans l'application Microsoft Office sur les systèmes d'exploitation dotés de l'Antimalware Scan Interface (AMSI). Vous pouvez autoriser ou interdire l'exécution d'un script considéré comme dangereux ou probablement dangereux. Si Kaspersky Security for Windows Server considère un script comme potentiellement dangereux, il exécute l'action que vous avez choisie : interdiction ou autorisation de l'exécution de ce script. Si vous avez choisi l'action **Interdire**, l'application autorise l'exécution du script uniquement si ce script ne présente aucun danger.

A partir du système d'exploitation Microsoft Windows Server 2016, Kaspersky Security for Windows Server prend en charge l'Antimalware Scan Interface (AMSI). La technologie AMSI permet l'intégration d'applications et de services à n'importe quelle application antimalware installée sur un ordinateur afin que cette application puisse intercepter et analyser tous les scripts exécutés.

Le module Monitoring des scripts n'est pas installé par défaut sur le serveur car l'exécution de cette tâche peut provoquer des erreurs de serveur. Quand le composant Monitoring des scripts est installé, l'application est enregistrée en tant que fournisseur AMSI et commence à surveiller les scripts exécutés.

Sur les ordinateurs tournant sous des systèmes d'exploitation qui ne sont pas compatible avec la fonction AMSI, l'utilisation de ce composant peut être incompatible avec certaines applications tierces installées sur le serveur protégé. Dans ce cas, le monitoring des scripts tiers peut donner lieu à des erreurs de fonctionnement des scripts. Il est recommandé de ne pas utiliser de telles applications tierces ou de désactiver la tâche Monitoring des scripts. Si la tâche est désactivée, les risques associés à la sécurité d'exécution des scripts augmente.

Si vous souhaitez utiliser le module Monitoring des scripts, il faut le sélectionner manuellement dans la liste des modules à installer lors de l'installation de Kaspersky Security for Windows Server. Si le composant est installé, la tâche Monitoring des scripts est lancée automatiquement par défaut au lancement de Kaspersky Security for



Windows Server.

Pour obtenir les détails relatifs à la sélection des modules de l'application lors de l'installation, consultez les *chapitres consacrés à l'installation dans le Manuel de l'administrateur de Kaspersky Security for Windows Server*.

Pour obtenir de plus amples informations sur la fonction AMSI, consultez le site de Microsoft Windows <https://docs.microsoft.com/en-us/windows/desktop/amsi/antimalware-scan-interface-portal>.

Vous pouvez configurer les paramètres de la tâche Monitoring des scripts (cf. section "Configuration des paramètres de la tâche Monitoring des scripts via la Console de l'application" à la page [292](#)).

## Paramètres par défaut de la tâche Monitoring des scripts

La tâche système Monitoring des scripts possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 44. Paramètres par défaut de la tâche Monitoring des scripts

Paramètre	Valeur par défaut	Description
Action à exécuter sur les scripts dangereux	<b>Interdire</b>	Vous pouvez indiquer les actions à effectuer en cas de détection de scripts potentiellement dangereux : interdire ou autoriser leur exécution.
Analyse heuristique	Le niveau de sécurité <b>Moyenne</b> est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Zone de confiance	Appliquée	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.

## Configuration des paramètres de la tâche Monitoring des scripts via le Plug-in d'administration

► *Pour configurer la tâche Monitoring des scripts, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une

stratégie" à la page [123](#)).

- Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel du serveur** de la fenêtre **Propriétés : <nom de la stratégie>**, cliquez sur **Configuration** pour **Monitoring des scripts**.
5. Dans la section **Actions à exécuter sur les scripts dangereux** de l'onglet **Général**, réalisez une des opérations suivantes :
  - Si vous souhaitez autoriser l'exécution des scripts présumés dangereux, sélectionnez l'option **Autoriser**.  
Kaspersky Security for Windows Server autorise l'exécution d'un script potentiellement dangereux.
  - Si vous souhaitez interdire l'exécution des scripts présumés dangereux, sélectionnez l'option **Interdire**.  
Kaspersky Security for Windows Server interdit l'exécution d'un script potentiellement dangereux.  
Cette option est sélectionnée par défaut.
6. Dans la section **Analyse heuristique**, réalisez une des opérations suivantes :
  - Cochez ou décochez la case **Utiliser l'analyse heuristique**.  
La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.  
Si la case est cochée, l'analyse heuristique est activée.  
Si la case est décochée, l'analyse heuristique est désactivée.  
Cette case est cochée par défaut.
  - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.  
Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.  
Il existe trois niveaux de détail pour l'analyse
    - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
    - **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.  
Il s'agit du niveau par défaut.

- **Minutieuse.** L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

7. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server tiendra compte des exclusions définie en fonction de leur emplacement et/ou d'un objet détecté par nom ou masque de nom dans la liste d'exclusions de la zone de confiance.

Si la case est décochée, Kaspersky Security for Windows Server ignore les exclusions dans la tâche Monitoring des scripts.

Cette case est cochée par défaut.

8. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis sont appliqués

## Configuration des paramètres de la tâche Monitoring des scripts via la Console de l'application

► *Pour configurer la tâche Monitoring des scripts, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Monitoring des scripts**.
3. Cliquez sur le lien **Propriétés** dans le panneau de détails du nœud.

La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.

4. Dans la section **Actions à exécuter sur les scripts dangereux**, réalisez une des opérations suivantes :

- Si vous souhaitez autoriser l'exécution des scripts présumés dangereux, sélectionnez l'option **Autoriser**.

Kaspersky Security for Windows Server autorise l'exécution d'un script potentiellement dangereux.

- Si vous souhaitez interdire l'exécution des scripts présumés dangereux, sélectionnez l'option **Interdire**.

Kaspersky Security for Windows Server interdit l'exécution d'un script potentiellement dangereux.

Cette option est sélectionnée par défaut.

5. Dans la section **Analyse heuristique**, réalisez une des opérations suivantes :

- Cochez ou décochez la case **Utiliser l'analyse heuristique**.

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

- Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

Il existe trois niveaux de détail pour l'analyse

- **Superficielle.** L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
- **Moyenne.** L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.

Il s'agit du niveau par défaut.

- **Minutieuse.** L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

6. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server tiendra compte des exclusions définies en fonction de leur emplacement et/ou d'un objet détecté par nom ou masque de nom dans la liste d'exclusions de la zone de confiance.

Si la case est décochée, Kaspersky Security for Windows Server ignore les exclusions dans la tâche Monitoring des scripts.

Cette case est cochée par défaut.

7. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis sont appliqués

## Statistiques de la tâche Monitoring des scripts

Au cours de l'exécution de la tâche Monitoring des scripts, vous pouvez consulter les informations sur la quantité de scripts que Kaspersky Security for Windows Server a traités entre le lancement de la tâche et le moment présent.

► *Pour consulter les statistiques de la tâche Monitoring des scripts, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Monitoring des scripts**.

Les statistiques de la tâche en cours sont affichées dans le volet des détails du nœud dans les sections

**Administration et Statistiques.**

Vous pouvez consulter les informations sur les objets que Kaspersky Security for Windows Server a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 45. Statistiques de la tâche Monitoring des scripts

Champ	Description
<b>Scripts bloqués</b>	Nombre de scripts dont l'exécution a été interdite par Kaspersky Security for Windows Server.
<b>Scripts dangereux détectés</b>	Nombre de scripts dangereux découverts.
<b>Scripts présumés dangereux détectés</b>	Nombre de scripts potentiellement dangereux découverts.
<b>Scripts traités</b>	Nombre total de scripts traités.

# Utilisation du KSN

Cette section contient des informations sur la tâche Utilisation du KSN et les instructions sur la configuration de cette tâche.

## Contenu du chapitre

A propos de la tâche Utilisation du KSN.....	<a href="#">295</a>
Paramètres de la tâche Utilisation du KSN par défaut .....	<a href="#">297</a>
Administration de l'utilisation du KSN via le plug-in d'administration .....	<a href="#">297</a>
Administration de l'utilisation du KSN via la Console de l'application .....	<a href="#">302</a>
Configuration du transfert de données supplémentaires.....	<a href="#">306</a>
Statistiques de la tâche Utilisation du KSN .....	<a href="#">307</a>

## A propos de la tâche Utilisation du KSN

*Kaspersky Security Network* (ci-après, "KSN") est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab concernant la réputation des fichiers, des ressources Internet et des applications. L'utilisation des données du Kaspersky Security Network assure une vitesse de réaction plus élevée de Kaspersky Security for Windows Server face aux nouvelles menaces, augmente l'efficacité de certains modules de la protection et réduit la possibilité de faux positifs.

**Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.**

Kaspersky Security for Windows Server obtient uniquement du Kaspersky Security Network les informations sur la réputation des applications.

La participation des utilisateurs au KSN permet à Kaspersky Lab d'obtenir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des outils de neutralisation et de réduire le nombre de faux positifs des modules de l'application.

Pour de plus amples informations sur le transfert, le traitement, le stockage et la destruction des informations sur l'utilisation de l'application, vous pouvez consulter la fenêtre Traitement des données de la tâche Utilisation du KSN et la Politique de confidentialité sur le site Internet de Kaspersky Lab.

La participation au Kaspersky Security Network est volontaire. La décision de participer à Kaspersky Security Network est prise pendant ou après l'installation de Kaspersky Security for Windows Server. Vous pouvez changer

d'avis quant à votre décision de participer au Kaspersky Security Network à n'importe quel moment.

Le réseau Kaspersky Security Network peut être utilisé dans les tâches suivantes de Kaspersky Security for Windows Server :

- Protection des fichiers en temps réel.
- Analyse à la demande.
- Contrôle du lancement des applications.
- Protection du trafic.
- Protection RPC des stockages réseau connectés.
- Protection ICAP des stockages réseau connectés.

### Kaspersky Private Security Network

Vous trouverez toutes les informations détaillées sur la configuration de Private Security Network (ci-après "KSN privé") dans l'aide de Kaspersky Security Center.

Si vous utilisez le KSN privé sur le serveur protégé, dans la fenêtre **Traitement des données** (cf. section "Configuration du traitement des données via le Plug-in d'administration" à la page [299](#)) de la tâche Utilisation du KSN, vous pouvez lire la Déclaration de KSN et activer la tâche en cochant la case **Accepter la Déclaration du Kaspersky Private Security Network**. En acceptant les conditions, vous acceptez d'envoyer tous types de données mentionnées dans la Déclaration de KSN (demandes de sécurité, données statistiques) aux services KSN.

Quand vous avez accepté les conditions du KSN privé, les cases qui règlent l'utilisation du KSN global sont indisponibles.

Si vous désactivez le KSN privé lorsque la tâche Utilisation du KSN est en cours d'exécution, l'erreur *Violation de la licence* se produit et la tâche s'arrête. Pour continuer à protéger le serveur, vous devez accepter manuellement la Déclaration de KSN sous l'onglet **Traitement des données** et relancer la tâche.

### Annulation de l'acceptation de la Déclaration de KSN

Vous pouvez annuler l'acceptation et arrêter tout échange de données avec Kaspersky Security Network à n'importe quel moment. Les actions suivantes sont considérées comme l'annulation complète ou partielle de la Déclaration de KSN :

- Si vous décochez la case **Envoyer des données sur les fichiers analysés**, l'application arrête d'envoyer des sommes de contrôle des fichiers analysés au service KSN pour analyse.
- En décochant la case **Envoyer des données relatives aux URL analysées** : l'application n'envoie plus les URL pour analyse.
- Si vous décochez la case **Envoyer les statistiques de Kaspersky Security Network**, l'application arrête de traiter des données avec des statistiques KSN supplémentaires.
- Si vous décochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Security Network**, l'application arrête le traitement de toutes les données liées à KSN et la tâche Utilisation du KSN s'arrête.
- En décochant la case **J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection** :

le service KMP est désactivé.

- Désinstallation du composant Utilisation du KSN : le traitement de toutes les données liées à KSN s'arrête.
- Désinstallation de Kaspersky Security for Windows Server via Kaspersky Security Center : le traitement de toutes les données liées à KSN s'arrête.

## Paramètres de la tâche Utilisation du KSN par défaut

Vous pouvez modifier les paramètres de la tâche Utilisation du KSN précisés par défaut (cf. tableau ci-dessous).

Tableau 46. Paramètres de la tâche Utilisation du KSN par défaut

Paramètre	Valeur par défaut	Description
<b>Actions à exécuter sur les objets douteux selon KSN</b>	Supprimer	Vous pouvez préciser les actions que Kaspersky Security for Windows Server va exécuter sur les objets réputés comme douteux par KSN.
<b>Transfert de données</b>	La somme de contrôle (hash MD5) est calculée pour les fichiers dont la taille ne dépasse pas 2 Mo.	Vous pouvez définir la taille maximale des fichiers dont la somme de contrôle sera calculée à l'aide de l'algorithme MD5 pour envoi à KSN. Si la case est décochée, Kaspersky Security for Windows Server calcule les hash MD5 pour les fichiers de n'importe quelle taille.
<b>Planification du lancement de la tâche</b>	Le premier lancement n'est pas défini.	Vous pouvez lancer la tâche manuellement ou planifier son exécution.

## Administration de l'utilisation du KSN via le plug-in d'administration

Cette section explique comment configurer la tâche Utilisation du KSN et le Traitement des données via le Plug-in d'administration.

### Dans cette section

Configuration de la tâche Utilisation du KSN via le plug-in d'administration .....	<a href="#">298</a>
Configuration du traitement des données via le plug-in d'administration .....	<a href="#">299</a>



## Configuration de la tâche Utilisation du KSN via le plug-in d'administration

► Pour configurer les paramètres de la tâche Utilisation du KSN, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Configuration** de la sous-section **Utilisation du KSN**.

La fenêtre **Utilisation du KSN** s'ouvre.

5. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :

- Dans la section **Actions à exécuter sur les objets douteux selon KSN**, indiquez l'action que Kaspersky Security for Windows Server doit exécuter en cas de détection d'un objet identifié comme infecté par le KSN :
  - **Supprimer**

Kaspersky Security for Windows Server supprime l'objet considéré comme douteux selon les données du KSN et place une copie de celui-ci dans la sauvegarde.

Cette option est sélectionnée par défaut.
  - **Consigner les informations**

Kaspersky Security for Windows Server consigne dans le journal d'exécution de la tâche les informations sur l'objet considéré comme douteux selon les données du KSN.

Kaspersky Security for Windows Server ne supprime pas l'objet douteux.
- Dans la section **Transfert de données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :
  - Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi à KSN si la taille du fichier est supérieure à (Mo)**.

La case active ou désactive le calcul de la somme de contrôle des fichiers d'une taille définie pour l'envoi de ces informations au service KSN.

La durée du calcul de la somme de contrôle dépend de la taille du fichier.

Si la case est cochée, Kaspersky Security for Windows Server ne calcule pas la somme de contrôle pour les fichiers dont la taille dépasse la valeur définie (Mo).

Si la case est décochée, Kaspersky Security for Windows Server calcule la somme de contrôle pour les fichiers de n'importe quelle taille.

Cette case est cochée par défaut.

- Le cas échéant, modifiez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Security for Windows Server calcule la somme de contrôle.
- Dans la section **Serveur proxy du KSN**, cochez ou décochez la case **Utiliser Kaspersky Security Center en tant que serveur proxy du KSN**.

La case permet d'administrer le transfert de données entre les serveurs protégés et KSN.

Si la case est décochée, les données du serveur d'administration et des serveurs protégés sont envoyées à KSN directement (et non via Kaspersky Security Center). La stratégie active définit le type de données qui peut être envoyé directement à KSN.

Si la case est cochée, toutes les données sont envoyées à KSN via Kaspersky Security Center.

Cette case est cochée par défaut.

Pour activer le proxy KSN, la Déclaration de KSN doit être acceptée et Kaspersky Security Center correctement configuré. Cf. *Système d'aide de Kaspersky Security Center* pour plus de détails.

6. Le cas échéant, configurez la planification du lancement de la tâche sous l'onglet **Administration des tâches**. Par exemple, vous pouvez démarrer la tâche planifiée et choisir la fréquence **Au lancement de l'application** si vous souhaitez que la tâche soit lancée automatiquement au redémarrage du serveur.  
L'application lancera la tâche Utilisation du KSN selon la planification.
7. Configurez le traitement des données (cf. section "Configuration du traitement des données via le Plug-in d'administration" à la page [299](#)) avant de lancer la tâche.
8. Cliquez sur le bouton **OK**.

Les modifications des paramètres de la tâche seront appliquées. La date et l'heure de modification des paramètres, ainsi que les informations sur les paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Configuration du traitement des données via le plug-in d'administration

Vous pouvez modifier les paramètres par défaut de traitement des données (cf. tableau ci-dessous).

Tableau 47. Paramètres par défaut de traitement des données

Paramètre	Valeur par défaut	Description
<b>J'accepte les dispositions de la Déclaration de Kaspersky Security Network</b>	Non cochée	Si cette option est sélectionnée, la participation à KSN après l'installation est acceptée. Vous pouvez modifier votre choix concernant l'utilisation du KSN à tout moment.
<b>Envoyer les statistiques de Kaspersky Security Network</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les statistiques de KSN seront envoyées automatiquement, sauf si vous décochez la case.
<b>Envoyer des données sur les fichiers analysés</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les données sur les fichiers précédemment analysés depuis le démarrage de la tâche sont envoyées. Il est possible de décocher la case à tout moment.
<b>Envoyer des données relatives aux URL analysées</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	En cas d'acceptation de la Déclaration de KSN, l'application envoie les informations relatives aux adresses Internet consultées à Kaspersky Lab.
<b>Accepter les dispositions de la Déclaration de Kaspersky Managed Protection</b>	Non cochée	Vous pouvez activer et désactiver l'application de n'importe quelle heuristique. Le service est disponible uniquement si l'accord séparé a été signé pendant le processus d'achat de l'application.

► Pour configurer les données qui seront traitées par les services KSN et accepter la déclaration de KSN, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel du serveur**, cliquez sur le bouton **Traitement des données** de la sous-section **Utilisation du KSN**.

La fenêtre **Traitement des données** s'ouvre.

5. Sous l'onglet **Statistiques et services**, lisez la Déclaration et cochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Security Network**.
6. Pour augmenter le niveau de protection, les cases suivantes sont automatiquement cochées :

- **Envoyer des données sur les fichiers analysés.**

Si la case est décochée, Kaspersky Security for Windows Server envoie la somme de contrôle des fichiers analysés à Kaspersky Lab. La conclusion sur la sécurité de chaque fichier est basée sur la réputation reçue de KSN.

Si la case est décochée, Kaspersky Security for Windows Server n'envoie pas la somme de contrôle des fichiers à KSN.

Remarque : les demandes concernant la réputation du fichier peuvent être envoyées en mode limité. Les limitations servent à la protection des serveurs de réputation Kaspersky Lab contre les DDoS. Dans ce scénario, les paramètres des demandes de réputation des fichiers, en cours d'envoi, sont définis par les règles et méthodes établies par les experts de Kaspersky Lab. L'utilisateur ne peut pas les configurer sur un ordinateur protégé. Les mises à jour de ces règles et méthodes sont reçues avec les mises à jour des bases de données de l'application. Si les limitations sont appliquées, l'état *Activé par Kaspersky Lab pour protéger les serveurs de KSN contre les attaques DDoS* apparaît dans les statistiques de la tâche Utilisation du KSN.

Cette case est cochée par défaut.

- **Envoyer des données relatives aux URL analysées.**

Si la case est cochée, Kaspersky Security for Windows Server envoie les données des ressources Internet demandées, y compris des adresses Internet à Kaspersky Lab. La conclusion sur la sécurité des ressources Internet demandées est basée sur la réputation reçue de KSN.

Si la case est décochée, Kaspersky Security for Windows Server n'obtient pas les informations relatives à la réputation des adresses Internet depuis le KSN.

Cette case est cochée par défaut.

La case a une influence sur la configuration de la tâche Protection du trafic.

Vous pouvez décocher ces cases et arrêter d'envoyer des données supplémentaires à tout moment.

7. La case **Envoyer les statistiques de Kaspersky Security Network** est cochée par défaut. Vous pouvez décocher la case à tout moment si vous ne souhaitez pas que Kaspersky Security for Windows Server envoie des statistiques complémentaires à Kaspersky Lab.

Si la case est cochée, Kaspersky Security for Windows Server envoie des statistiques supplémentaires qui peuvent contenir des données personnelles. La liste de toutes les données envoyées comme des statistiques KSN sont spécifiées dans la Déclaration de KSN. Les données reçues par Kaspersky Lab servent à améliorer la qualité des applications et le niveau des taux de détection des menaces.

Si la case est décochée, Kaspersky Security for Windows Server n'envoie pas de statistiques supplémentaires.

Cette case est cochée par défaut.

8. Sous l'onglet **Kaspersky Managed Protection**, lisez la Déclaration et cochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection**.

Si la case est cochée, vous acceptez d'envoyer les statistiques sur l'activité du serveur protégé aux spécialistes de Kaspersky Lab. Les données reçues sont utilisées pour l'analyse et la génération de rapports 24h/24 requises afin d'éviter les incidents liées à une violation de sécurité.

Cette case est décochée par défaut.

Les changements d'état de la case **J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection** ne démarrent ou n'arrêtent pas immédiatement le traitement des données. Pour appliquer les changements, vous devez redémarrer Kaspersky Security for Windows Server.

Pour utiliser le service KMP, vous devez signer le contrat correspondant et exécuter les fichiers de configuration sur un serveur protégé, et cocher les cases **J'accepte les dispositions de la Déclaration de Kaspersky Security Network**, **Envoyer des données sur les fichiers analysés**, **Envoyer des données relatives aux URL analysées**, et **Envoyer les statistiques de Kaspersky Security Network** sous l'onglet **Statistiques et services**.

9. Cliquez sur le bouton **OK**.

La configuration du traitement des données sera enregistrée.

## Administration de l'utilisation du KSN via la Console de l'application

Cette section explique comment configurer la tâche Utilisation du KSN et le Traitement des données via la Console de l'application.

### Dans cette section

Configuration de la tâche Utilisation du KSN via la Console de l'application .....	<a href="#">302</a>
Configuration du traitement des données via la Console de l'application .....	<a href="#">304</a>

## Configuration de la tâche Utilisation du KSN via la Console de l'application

► Pour configurer les paramètres de la tâche Utilisation du KSN, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.

2. Sélectionnez le nœud enfant **Utilisation du KSN**.
3. Dans le panneau de résultats, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.

4. Configurez les paramètres de la tâche :
  - Dans la section **Actions à exécuter sur les objets douteux selon KSN**, indiquez l'action que Kaspersky Security for Windows Server doit exécuter en cas de détection d'un objet identifié comme infecté par le KSN :

- **Supprimer**

Kaspersky Security for Windows Server supprime l'objet considéré comme douteux selon les données du KSN et place une copie de celui-ci dans la sauvegarde.

Cette option est sélectionnée par défaut.

- **Consigner les informations**

Kaspersky Security for Windows Server consigne dans le journal d'exécution de la tâche les informations sur l'objet considéré comme douteux selon les données du KSN.

Kaspersky Security for Windows Server ne supprime pas l'objet douteux.

- Dans la section **Transfert de données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :

- Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi à KSN si la taille du fichier est supérieure à (Mo)**.

La case active ou désactive le calcul de la somme de contrôle des fichiers d'une taille définie pour l'envoi de ces informations au service KSN.

La durée du calcul de la somme de contrôle dépend de la taille du fichier.

Si la case est cochée, Kaspersky Security for Windows Server ne calcule pas la somme de contrôle pour les fichiers dont la taille dépasse la valeur définie (Mo).

Si la case est décochée, Kaspersky Security for Windows Server calcule la somme de contrôle pour les fichiers de n'importe quelle taille.

Cette case est cochée par défaut.

- Le cas échéant, modifiez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Security for Windows Server calcule la somme de contrôle.

5. Le cas échéant, configurez la planification du lancement de la tâche sous les onglets **Planification** et **Avancé**. Par exemple, vous pouvez activer le lancement d'une tâche planifiée et choisir la fréquence de lancement **Au lancement de l'application** si vous souhaitez que la tâche soit lancée automatiquement après le redémarrage du serveur.

L'application lancera la tâche Utilisation du KSN selon la planification.

6. Configurez le traitement des données (cf. section "Configuration du traitement des données via la Console de l'application" à la page [304](#)) avant de lancer la tâche.

7. Cliquez sur le bouton **OK**.

Les modifications des paramètres de la tâche seront appliquées. La date et l'heure de modification des paramètres, ainsi que les informations sur les paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Configuration du traitement des données via la Console de l'application

Vous pouvez modifier les paramètres par défaut de traitement des données (cf. tableau ci-dessous).

Tableau 48. Paramètres par défaut de traitement des données

Paramètre	Valeur par défaut	Description
<b>J'accepte les dispositions de la Déclaration de Kaspersky Security Network</b>	Non cochée	Si cette option est sélectionnée, la participation à KSN après l'installation est acceptée. Vous pouvez modifier votre choix concernant l'utilisation du KSN à tout moment.
<b>Envoyer les statistiques de Kaspersky Security Network</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les statistiques de KSN seront envoyées automatiquement, sauf si vous décochez la case.
<b>Envoyer des données sur les fichiers analysés</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les données sur les fichiers précédemment analysés depuis le démarrage de la tâche sont envoyées. Il est possible de décocher la case à tout moment.
<b>Envoyer des données relatives aux URL analysées</b>	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	En cas d'acceptation de la Déclaration de KSN, l'application envoie les informations relatives aux adresses Internet consultées à Kaspersky Lab.
<b>Accepter les dispositions de la Déclaration de Kaspersky Managed Protection</b>	Non cochée	Vous pouvez activer et désactiver l'application de n'importe quelle heuristique. Le service est disponible uniquement si l'accord séparé a été signé pendant le processus d'achat de l'application.

► Pour configurer les données qui seront traitées par les services KSN et accepter la déclaration de KSN, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Utilisation du KSN**.
3. Dans le panneau de détails, cliquez sur le lien **Traitement des données**.  
La fenêtre **Traitement des données** s'ouvre.
4. Sous l'onglet **Statistiques et services**, lisez la Déclaration et cochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Security Network**.
5. Pour augmenter le niveau de protection, les cases suivantes sont automatiquement cochées :
  - **Envoyer des données sur les fichiers analysés**.

Si la case est décochée, Kaspersky Security for Windows Server envoie la somme de contrôle des fichiers analysés à Kaspersky Lab. La conclusion sur la sécurité de chaque



fichier est basée sur la réputation reçue de KSN.

Si la case est décochée, Kaspersky Security for Windows Server n'envoie pas la somme de contrôle des fichiers à KSN.

Remarque : les demandes concernant la réputation du fichier peuvent être envoyées en mode limité. Les limitations servent à la protection des serveurs de réputation Kaspersky Lab contre les DDoS. Dans ce scénario, les paramètres des demandes de réputation des fichiers, en cours d'envoi, sont définis par les règles et méthodes établies par les experts de Kaspersky Lab. L'utilisateur ne peut pas les configurer sur un ordinateur protégé. Les mises à jour de ces règles et méthodes sont reçues avec les mises à jour des bases de données de l'application. Si les limitations sont appliquées, l'état *Activé par Kaspersky Lab pour protéger les serveurs de KSN contre les attaques DDoS* apparaît dans les statistiques de la tâche Utilisation du KSN.

Cette case est cochée par défaut.

- **Envoyer des données relatives aux URL analysées.**

Si la case est cochée, Kaspersky Security for Windows Server envoie les données des ressources Internet demandées, y compris des adresses Internet à Kaspersky Lab. La conclusion sur la sécurité des ressources Internet demandées est basée sur la réputation reçue de KSN.

Si la case est décochée, Kaspersky Security for Windows Server n'obtient pas les informations relatives à la réputation des adresses Internet depuis le KSN.

Cette case est cochée par défaut.

La case a une influence sur la configuration de la tâche Protection du trafic.

Vous pouvez décocher ces cases et arrêter d'envoyer des données supplémentaires à tout moment.

6. La case **Envoyer les statistiques de Kaspersky Security Network** est cochée par défaut. Vous pouvez décocher la case à tout moment si vous ne souhaitez pas que Kaspersky Security for Windows Server envoie des statistiques complémentaires à Kaspersky Lab.

Si la case est cochée, Kaspersky Security for Windows Server envoie des statistiques supplémentaires qui peuvent contenir des données personnelles. La liste de toutes les données envoyées comme des statistiques KSN sont spécifiées dans la Déclaration de KSN. Les données reçues par Kaspersky Lab servent à améliorer la qualité des applications et le niveau des taux de détection des menaces.

Si la case est décochée, Kaspersky Security for Windows Server n'envoie pas de statistiques supplémentaires.

Cette case est cochée par défaut.

7. Sous l'onglet **Kaspersky Managed Protection**, lisez la Déclaration et cochez la case **J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection**.

Si la case est cochée, vous acceptez d'envoyer les statistiques sur l'activité du serveur protégé aux spécialistes de Kaspersky Lab. Les données reçues sont utilisées pour l'analyse et la génération de rapports 24h/24 requises afin d'éviter les incidents liés à une violation de sécurité.

Cette case est décochée par défaut.



Les changements d'état de la case **J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection** ne démarrent ou n'arrêtent pas immédiatement le traitement des données. Pour appliquer les changements, vous devez redémarrer Kaspersky Security for Windows Server.

Pour utiliser le service KMP, vous devez signer le contrat correspondant et exécuter les fichiers de configuration sur un serveur protégé, et cocher les cases **J'accepte les dispositions de la Déclaration de Kaspersky Security Network, Envoyer des données sur les fichiers analysés, Envoyer des données relatives aux URL analysées, et Envoyer les statistiques de Kaspersky Security Network** sous l'onglet **Statistiques et services**.

8. Cliquez sur le bouton **OK**.

La configuration du traitement des données sera enregistrée.

## Configuration du transfert de données supplémentaires

Kaspersky Security for Windows Server peut être configuré pour envoyer à Kaspersky Lab les données suivantes :

- Sommes de contrôle des fichiers analysés (case **Envoyer des données sur les fichiers analysés**).
- Données relatives aux adresses Internet traitées et aux emails traités (case **Envoyer des données relatives aux URL analysées**).
- Statistiques supplémentaires, y compris des données personnelles (case **Envoyer les statistiques de Kaspersky Security Network**).

Consultez la section « **Traitement des données locales** » de ce manuel pour plus d'information sur les données envoyées à Kaspersky Lab.

Les cases correspondantes peuvent être cochées ou décochées (cf. section "Configuration du traitement des données via la Console de l'application" à la page [304](#)) uniquement si la case **J'accepte les dispositions de la Déclaration de Kaspersky Security Network** est cochée.

Par défaut, Kaspersky Security for Windows Server calcule les sommes de contrôle des fichiers et des statistiques supplémentaires après l'acceptation de la Déclaration de KSN.

Tableau 49. Etats possibles de la case à cocher et conditions correspondante

Etat de la case	Conditions pour l'état de la case Envoyer des données sur les fichiers analysés.	Conditions pour l'état de la case Envoyer les statistiques de Kaspersky Security Network	Conditions pour l'état de la case Envoyer des données sur les URL analysées	Conditions pour l'état de la case J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection	Conditions pour l'état de la case J'accepte les dispositions de la Déclaration de Kaspersky Security Network

Etat de la case	Conditions pour l'état de la case Envoyer des données sur les fichiers analysés.	Conditions pour l'état de la case Envoyer les statistiques de Kaspersky Security Network	Conditions pour l'état de la case Envoyer des données sur les URL analysées	Conditions pour l'état de la case J'accepte les dispositions de la Déclaration de Kaspersky Managed Protection	Conditions pour l'état de la case J'accepte les dispositions de la Déclaration de Kaspersky Security Network
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> <li>Des demandes sur la réputation sont envoyées</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Des statistiques supplémentaires sont envoyées</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Des statistiques supplémentaires sont envoyées</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Des statistiques supplémentaires sont envoyées</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Des statistiques supplémentaires sont envoyées</li> <li>Case modifiable</li> </ul>
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> <li>Aucune demande sur la réputation n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>Aucune demande sur la réputation n'est envoyée</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case modifiable</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>Aucune demande sur la réputation n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>	<ul style="list-style-type: none"> <li>Aucune statistique supplémentaire n'est envoyée</li> <li>Case non modifiable</li> </ul>

## Statistiques de la tâche Utilisation du KSN

Pendant l'exécution de la tâche Utilisation du KSN, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security for Windows Server depuis son lancement jusqu'à maintenant. Les informations relatives à tous les événements survenus pendant l'exécution d'une tâche sont consignés dans le journal d'exécution de la tâche (cf. section "A propos des journaux d'exécution des tâches" à la page [216](#)).

► Pour consulter les statistiques de la tâche Utilisation du KSN, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Utilisation du KSN**.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Vous pouvez consulter les informations sur les objets que Kaspersky Security for Windows Server a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 50. Statistiques de la tâche Utilisation du KSN

Champ	Description
<b>Requêtes fichier envoyées</b>	Nombre de requêtes sur la réputation de fichiers que Kaspersky Security for Windows Server a envoyées au KSN.
<b>Requêtes d'adresse Internet envoyées</b>	Nombre de requêtes sur la réputation d'adresses Internet que Kaspersky Security for Windows Server a envoyées à KSN.
<b>URL douteuses dans KSN</b>	Nombre d'URL considérées comme douteuses par KSN.
<b>Fichiers douteux dans KSN</b>	Nombre d'objets considérés comme douteux par KSN.
<b>Erreurs d'envoi des requêtes</b>	Nombre de requêtes à KSN dont le traitement a entraîné une erreur de tâche.
<b>Statistiques collectées</b>	Nombre de paquets de statistiques générés envoyés à KSN.
<b>Objets supprimés</b>	Nombre d'objets que Kaspersky Security for Windows Server a supprimés suite au fonctionnement de la tâche Utilisation du KSN.
<b>Objets sauvegardés</b>	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security for Windows Server.
<b>Objets non supprimés</b>	Nombre d'objets que Kaspersky Security for Windows Server a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.
<b>Objets non sauvegardés</b>	Nombre d'objets dont Kaspersky Security for Windows Server a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque. L'application ne désinfecte pas et ne supprime pas les fichiers qui n'ont pas pu être placés dans la sauvegarde. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.
<b>Mode limité</b>	L'état indique si l'application envoie des requêtes sur la réputation des fichiers en mode limité.

# Protection du trafic

Cette section contient des informations sur la tâche Protection du trafic et les instructions sur la configuration de cette tâche.

## Contenu du chapitre

A propos de la tâche Protection du trafic.....	<a href="#">309</a>
A propos des règles de protection du trafic .....	<a href="#">310</a>
Protection contre les menaces email.....	<a href="#">311</a>
Liste des catégories.....	<a href="#">312</a>
Paramètres de niveau de protection prédéfini.....	<a href="#">316</a>
Paramètres par défaut de la tâche Protection du trafic .....	<a href="#">317</a>
Administration de la Protection du trafic via le plug-in d'administration .....	<a href="#">318</a>
Administration de la protection du trafic via la Console de l'application.....	<a href="#">333</a>

## A propos de la tâche Protection du trafic

Le module Protection du trafic traite le trafic Internet (y compris le trafic obtenu via les services de messagerie) et intercepte et analyse les objets transmis via le trafic Internet afin de détecter les menaces informations connues ou autres sur le serveur protégé. Le service ICAP analyse le trafic entrant à la recherche de menaces et bloque ou autorise le trafic en fonction des résultats de l'analyse et des paramètres définis.

Kaspersky Security for Windows Server détecte aussi le trafic demandé par les processus exécutés sous Windows Subsystem for Linux. Pour ces processus, la tâche Protection du trafic applique l'action définie par la configuration de la tâche en cours.

La Protection du trafic est installée par défaut. Quand l'installation est terminée, les services suivants sont enregistrés et lancés :

- Service Protection contre les exploits de Kaspersky Security (KAVFSWH)

Le module offre les types de protection suivants :

- Protection contre les menaces email :
  - Anti-phishing
  - Protection contre les applications malveillantes transmises par messagerie :
- Protection contre les menaces Internet :
  - Anti-phishing
  - Analyse des adresses Internet malveillante
  - Protection contre les applications malveillantes sur Internet :

- Contrôle Internet :
  - Contrôle des URL
  - Contrôle des certificats
  - Contrôle Internet basé sur les catégories

Il est fortement recommandé d'utiliser les services KSN lors du démarrage de la tâche Protection du trafic pour améliorer la détection des menaces. Les bases de données cloud KSN contiennent davantage de données réelles sur les menaces Internet que les bases antivirus locales. L'analyse d'un certain nombre de catégories de contrôle Internet est uniquement basée sur les conclusions reçues des services KSN.

### Modes de la Protection du trafic

Protection du trafic peut fonctionner dans un des modes suivants :

- **Intercepteur de pilote.** L'application intercepte le trafic à l'aide d'un pilote réseau. Elle utilise un pilote noyau réseau pour intercepter et analyser tout le trafic entrant sur les ports indiqués.
- **Redirection.** L'application traite les demandes provenant du navigateur Internet de l'utilisateur comme serveur proxy et réachemine le trafic reçu sur un serveur ICAP interne. Ce mode implique une configuration supplémentaire du navigateur Internet : il est nécessaire de spécifier l'adresse et le port de la connexion du serveur proxy.
- **Proxy externe.** L'application traite le trafic depuis un serveur proxy externe. Le trafic est transmis depuis le serveur proxy externe vers Kaspersky Security for Windows Server. L'application analyse le trafic et recommande une action au serveur proxy. Kaspersky Security for Windows Server est compatible uniquement avec les proxys qui transfèrent le trafic via le protocole ICAP.

## A propos des règles de protection du trafic

Kaspersky Security for Windows Server permet d'ajouter et de configurer des règles d'autorisation ou d'interdiction pour les certificats et les adresses Internet. Il prend également en charge l'utilisation de catégories prédéfinies pour bloquer le contenu indésirable. Vous pouvez appliquer des règles pour les certificats si la tâche est exécutée dans le mode **Intercepteur de pilote** ou **Redirection** mode.

### Contrôle Internet

Ce type de contrôle est réalisé en appliquant des règles d'autorisation ou d'interdiction pour les adresses Internet et les certificats. Les règles d'autorisation ont priorité sur les conclusions du KSN et sur l'analyse à l'aide des signatures.

Il est possible d'autoriser ou d'interdire une adresse Internet ou un certificat sur la base de conclusions par ordre de priorité (de la priorité la plus haute à la plus basse) :

1. Règles d'autorisation ou d'interdiction.
2. Bases antivirus ou d'Anti-phishing.
3. KSN.
4. Catégorie.

## Contrôle Internet basé sur les catégories

Kaspersky Security for Windows Server permet de bloquer des adresses Internet en fonction de catégories. Vous pouvez définir le niveau d'analyse heuristique qui intervient dans la définition des catégories. Le contrôle Internet basé sur les catégories repose sur une liste prédéfinie de catégories pour l'analyse. Alors que la liste en elle-même ne peut pas être modifiée, il est possible de sélectionner les catégories des ressources Internet à autoriser ou à interdire, voire de désactiver le contrôle sur la base de catégorie. La catégorie Autre reprend toutes les ressources Internet qui n'appartiennent à aucune des autres catégories de la liste. Si la case est cochée, Kaspersky Security for Windows Server autorise toutes les ressources Internet qui n'appartiennent pas à une catégorie. Si la case est décochée, aucune ressource Internet n'est autorisée.

La définition de catégorie possède la priorité la plus faible.

Kaspersky Security for Windows Server applique seulement une règle par défaut : la règle d'interdiction pour les certificats TOR. Vous pouvez décocher la règle dans les paramètres de règle pour autoriser les connexions TOR. Si la règle est appliquée, toutes les connexions TOR entrantes et sortantes sont bloquées. Si la règle est appliquée, toutes les connexions TOR entrantes et sortantes sont bloquées.

La Protection du trafic considère également les conclusions pour un masque `not-a-virus` qui portent sur les ressources ou les objets qui ne sont pas des virus en tant que tels mais qui sont capables de nuire au serveur protégé. Par défaut, Kaspersky Security for Windows Server n'applique pas le masque `not-a-virus` aux catégories (cf. section "Configuration du Contrôle Internet basé sur les catégories" à la page [331](#)) "Configuration du Contrôle Internet basé sur les catégories" à la page [345](#)).

## Protection contre les menaces email

Le module Protection du trafic analyse le courrier dans Microsoft Outlook (2010, 2013 et 32 bits et 64 bits). La protection contre les menaces email est garantie via le Plug-in Microsoft Outlook installé en plus des modules de Kaspersky Security for Windows Server.

Protection contre les menaces email inclut les fonctions suivantes :

- Analyse des emails entrants et sortants.
- Recherche de virus dans les emails.
- Recherche de virus dans les pièces jointes (objets compactés compris).
- Analyse anti-phishing des emails.
- Analyse anti-phishing des objets compactés.

En cas de détection d'une menace, Kaspersky Security for Windows Server :

- Supprime définitivement les pièces jointes infectées.
- Modifie le corps du message infecté. Dans ce cas, l'original du corps du message infecté est joint comme page html avec les informations sur la menace. Si un lien de phishing est détecté, l'original du corps du message infecté est joint au format TXT avec les informations sur la menace.
- Enregistre un événement *Détection de menace*.

Kaspersky Security for Windows Server analyse les emails à l'ouverture de ceux-ci et non pas lorsqu'ils sont reçus par le serveur. L'analyse est réalisée une fois seulement à la première ouverture. Les emails et les objets

compactés analysés sont stockés dans le cache jusqu'au redémarrage d'Outlook. Après le redémarrage, tous les emails sont à nouveau analysés à l'ouverture.

► *Le Plug-in est chargé dans le client de messagerie Microsoft Outlook lors du démarrage. Si vous installez le Plug-in Microsoft Outlook tandis qu'Outlook est en cours d'exécution :*

1. Ouvrez **Fichier > Options > Plug-ins**.
2. Assurez-vous que le Plug-in Microsoft Outlook a été ajouté à une des listes (**actif** ou **inactif**).
3. Relancez Microsoft Outlook.
4. Vérifiez l'état du Plug-in Microsoft Outlook (doit devenir **Actif**).

## Liste des catégories

Les ressources Internet sont analysées et classées en catégories selon des tags. Le tag peut être appliqué à un certain nombre de catégorie (cf. tableau ci-dessous).

Tableau 51. *Tags pour les catégories de ressources Internet*

Tag	Description	Liste des catégories
18+ (adulte)	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu pour adultes (plus de 18 ans) comme des descriptions d'actes violents, de la pornographie ou du langage vulgaire.	Avortement, Rencontres entre adultes, Anorexie, Mécontentement, Discrimination, Erotique, Drogues illicites, Logiciels illicites, LGBT, Lingerie, Rencontres entre jeunes non adultes, Nudisme, Décision de police (JP), Porno, Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Education sexuelle, Réseaux sociaux, Suicide, Vocabulaire obscène, Violence, Armes.
enfants	Ces catégories peuvent contenir des ressources qui pourraient proposer du contenu pour les enfants. Par exemple, des sites Internet d'éducation, des sites de divertissements pour enfants, des forums et des blogs sur l'éducation des enfants.	Enfants, Limité par la Loi fédérale 436 (Féd. de Russie), Pages d'écoles et d'universités.
drogue	Ces catégories peuvent contenir des ressources qui pourraient proposer des informations sur les stupéfiants et autres substances licites ou illicites. Par exemple, des informations sur la distribution de drogues illicites ou d'alcool ou les sites Internet de sociétés pharmaceutiques enregistrées.	Avortement, Alcool, Anorexie, Drogue, Santé et beauté, Drogues illicites, Médecine, Pharmacie, Tabac.

Tag	Description	Liste des catégories
éducation	<p>Ces catégories peuvent contenir des ressources qui pourraient proposer du contenu pédagogique.</p> <p>Par exemple, des encyclopédies en ligne, des bases de connaissances, des sites wiki et des pages Internet de ressources éducatives ou des pages Internet consacrées à l'éducation sexuelle.</p>	<p>Livres et littérature, Enseignement, Enfants, Technologies de l'information, Encyclopédies en ligne, Pages d'écoles et d'universités, Moteurs de recherche, Education sexuelle.</p>
loisirs	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux loisirs, aux hobbies et aux activités récréatives.</p> <p>Par exemple, divers jeux en ligne, dont des sites de pari et les réseaux sociaux, des pages Internet sur la littérature ou la chasse, des blogs sur la santé et la beauté et des fils d'informations.</p>	<p>Rencontres pour adultes, Loisirs, Tous les supports de communication, Astrologie et ésotérisme, Audio, vidéo et logiciels, Paris, Blogs, Casinos, Jeux de cartes, Jeux occasionnels, Chats et forums, Jeux, Culture et société, Erotique, Mode, Partage de fichiers, Pêche et chasse, Enfants, Paris, Santé et beauté, Loisirs, Maison et famille, Humour, LGBT, Lingerie, Loteries, Hébergement et diffusion sur les médias, Médecine, Musique, Actualités, Rencontre entre jeunes non adultes, Nudisme, Boutiques en ligne, Boutiques en ligne (propre système de paiement), Animaux, Porno, Restaurants, café et alimentation, Sex shop, Réseaux sociaux, Sport, Torrents, Voyages, TV et radio, Jeux de guerre.</p>
jeux	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif à différents types de jeux. Par exemple, des jeux de hasard et des paris, des loteries, des jeux en ligne ou occasionnels ainsi que des sites et des forums consacrés aux jeux.</p>	<p>Jeux occasionnels, Jeux, Sport, Jeux de guerre.</p>
hasard	<p>Cette catégorie désigne les pages Internet contenant :</p> <p>Jeux de hasard payants.</p> <p>Paris.</p> <p>Loteries qui impliquent l'achat de billets/numéros de loterie.</p>	<p>Paris, Casinos, jeux de cartes, Jeux de hasard, Sport, Jeux de guerre.</p>
santé & médecine	<p>Pages Internet sur les modes de vie sains. Peuvent inclure des sites dédiés au fitness, à l'alimentation saine et à d'autres pratiques et méthodes de traitement ; pages Internet sur la médecine, la pharmacie, les sociétés pharmaceutiques et les médicaments et suppléments..</p>	<p>Avortement, Anorexie, Médicaments et drogues, Santé et beauté, Médecine, Pharmacie, Sport.</p>



Tag	Description	Liste des catégories
illicite	Ces catégories peuvent contenir des ressources Internet potentiellement illicites. Par exemple des sites de partage illégaux de fichiers musicaux/vidéo ou des pages Internet dont la visite est interdite par la législation de plusieurs pays.	Alcool, Audio, vidéo et logiciels, Drogues, Partage de fichiers, Drogues illicites, Logiciels illicites, Loteries, Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Tabac.
IT	Généralement, pages Internet qui permettent aux utilisateurs (avec ou sans la nécessité d'un compte) d'envoyer des messages personnels à d'autres utilisateurs (y compris des services email, des réseaux sociaux, des blogs, etc.)	Serveurs proxy anonymes, Services d'hébergement et de domaine, Logiciels illégaux, Technologies de l'information, Moteurs de recherche, Courrier Internet.
interdit par la loi	Ces catégories peuvent contenir des ressources Internet qui pourraient être soumises au contrôle de la législation fédérale ou qui pourraient être liées au gouvernement ou à la politique.	Législation et politique, Mentionné dans la Liste fédérale des extrémistes (Féd. de Russie), Limité par la Loi fédérale 436 (Féd. de Russie), Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie).
légal	Ces catégories peuvent contenir des ressources Internet potentiellement légales.	Alcool, Audio, vidéo et logiciels, Drogue, Partage de fichiers, Publicités licites, Loteries, Militaire, Pharmacie, Religion, Education sexuelle, Services de bandes-annonces et d'annonces, Tabac, Jeux de guerre.
partage de médias	Ces catégories peuvent reprendre des ressources Internet qui peuvent permettre le partage de fichiers. Par exemple, des torrents, des sites de partage de fichiers, des sites d'hébergement audio et vidéo, licites ou non.	Audio, vidéo et logiciels, Livres et littérature, Partage de fichiers, Enfants, Services Internet, Hébergement et diffusion sur les médias, Musique, Moteurs de recherche, Torrents, TV et radio
argent et paiement	Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux finances ou à des institutions financières. Par exemple, les sites Internet officiels de banques, des banques en ligne, des magasins en lignes et des pages Internet pour la réalisation de transferts d'argent.	Banques, Livres et littérature, Jeux occasionnels, E-commerce, Boutiques en ligne (propre système de paiement), Paiement par carte de crédit, Systèmes de paiement, Restaurants, cafés et alimentation, Voyages.

Tag	Description	Liste des catégories
collaboration en ligne	<p>Ces catégories peuvent contenir des ressources Internet concernant éventuellement aux communications en ligne.</p> <p>Par exemple, des blogs spécialisés et des forums, des chats privés, des réseaux sociaux ou des sites de rencontre.</p>	<p>Rencontres entre adultes, Blogs, Chats et forums, Enfants, Santé et beauté, Sites de recherche d'emploi, Médecine, Rencontres entre jeunes non adultes, Réseaux sociaux, Voyages.</p>
psychotrope & drogue	<p>Ces catégories peuvent contenir des ressources Internet associées à tous types de drogues, médicaments psychotropes ou produits à base de tabac.</p>	<p>Médicaments et drogues, Santé et beauté, Drogues illicites, Médecine, Pharmacie, Tabac.</p>
sexe & contenu pour adultes	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu à caractère sexuel ou érotique.</p> <p>Par exemple, des hébergeurs de pornographie, des pages Internet sur l'éducation sexuelle et des sites Internet sur les minorités sexuelles.</p>	<p>Rencontres entre adultes, Erotique, LGBT, Lingerie, Nudisme, Porno, Education sexuelle, Sex shops.</p>
société et droit	<p>Cette catégorie inclut de nombreux aspects de la société et de la vie humaine, y compris religion, associations religieuses, gouvernement, politique, lois, maison et famille, médias d'actualités, militaire et armes.</p>	<p>Culture et société, Droit et politique, Militaire, Religion, Armes.</p>
shopping	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient proposer du contenu relatif aux achats en ligne.</p>	<p>Livres et littérature, Lingerie, Boutiques en ligne, Boutiques en ligne (propre système de paiement), Paiement par carte de crédit, Restaurants, cafés et alimentation, Sex shops, Voyages.</p>
violence	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient présenter des expressions explicites d'agression, des descriptions d'actes de cruauté, de la propagande d'organisations extrémistes ou des descriptions de suicide.</p>	<p>Mécontentement, Discrimination, Extrémisme et racisme, Pêche et chasse, Haine et discrimination, Mentionné dans la Liste fédérale des extrémistes (Féd. de Russie), Militaire, Décision de police (JP), Limité par la législation mondiale, Limité par la législation (Féd. de Russie), Limité par Roskomnadzor (Féd. de Russie), Suicide, Violence, Jeux de guerre, Armes.</p>
service Internet	<p>Ces catégories peuvent contenir des ressources Internet qui pourraient proposer différents services Internet. Par exemple, des services d'anonymisation, d'hébergement de sites ou d'emails.</p>	<p>Serveurs proxy anonymes, Services d'hébergement et de domaine, Services Internet, Moteurs de recherche, Services de bandes-annonces et d'annonces, Courrier Internet.</p>

## Paramètres de niveau de protection prédéfini

Pour un nœud sélectionné dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez appliquer un des trois niveaux de protection prédéfinis suivants : Performance maximale, Recommandé et Protection maximale. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

### Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si des mesures de sécurité du serveur complémentaires ont été adoptées dans votre réseau, telles que des pare-feu ou des stratégies de sécurité, en plus de Kaspersky Security for Windows Server.

### Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

### Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité informatique élevé.

Tableau 52. Niveaux de protection prédéfinis et paramètres de sécurité correspondants

Options	Niveau de protection		
	Performance maximale	Recommandé	Protection maximale
<b>Analyser les objets</b>	Conformément à la liste des extensions dans la base de données	Tous les objets	Tous les objets
<b>Actions sur les objets infectés et autres objets détectés</b>	Interdire	Interdire	Interdire
<b>Ne pas détecter</b>	non	non	non
<b>Arrêter si l'analyse dure plus de (s.)</b>	60 s	60 s	60 s
<b>Ne pas analyser les objets de plus de (Mo)</b>	20 MB	20 MB	non

Options	Niveau de protection		
	Performance maximale	Recommandé	Protection maximale
<b>Protection des objets composés</b>	<ul style="list-style-type: none"> <li>Objets compactés*</li> </ul> <p>* uniquement les objets nouveaux et modifiés</p>	<ul style="list-style-type: none"> <li>Archives*</li> <li>Archives SFX*</li> <li>Objets compactés*</li> <li>Objets OLE intégrés*</li> </ul> <p>* uniquement les objets nouveaux et modifiés</p>	<ul style="list-style-type: none"> <li>Archives*</li> <li>Archives SFX*</li> <li>Objets compactés*</li> <li>Objets OLE intégrés*</li> </ul> <p>* Tous les objets</p>

## Paramètres par défaut de la tâche Protection du trafic

Vous pouvez modifier les paramètres de la tâche Protection du trafic par défaut (cf. tableau ci-dessous).

Tableau 53. Paramètres par défaut de la tâche Protection du trafic

Paramètre	Valeur par défaut	Description
<b>Mode de tâche</b>	Proxy externe	Le service ICAP traite le trafic depuis un serveur proxy externe.
<b>Numéro de port réseau</b>	1345	Le numéro de port par défaut pour le service ICAP.
<b>Identification du service</b>	Analyse Web	Identifiant du service ICAP pour l'adresse du serveur antivirus installé.
<b>Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes</b>	Appliquée.	Activez ou désactivez l'analyse de chaque adresse Internet à l'aide des signatures.
<b>Analyser les pages Internet à l'aide de la base de données anti-phishing</b>	Appliquée.	Activez ou désactivez l'analyse anti-phishing des adresses Internet à l'aide de l'analyse heuristique.
<b>Utiliser KSN pour la protection</b>	Appliquée.	Vous pouvez utiliser les données relatives à la réputation des applications de KSN pour garantir la protection lors de l'exécution de la tâche.
<b>Utiliser la zone de confiance</b>	Appliquée.	Vous pouvez appliquer la Zone de confiance si nécessaire.

Paramètre	Valeur par défaut	Description
<b>Niveau de protection</b>	Recommandé	Pour les entrées sélectionnées dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez : Appliquer un autre niveau de sécurité prédéfini ; Modifier manuellement le niveau de sécurité ;
<b>Planification du lancement de la tâche</b>	Le premier lancement n'est pas défini.	La tâche de protection du trafic sera lancée ou arrêtée. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

## Administration de la Protection du trafic via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des serveurs du réseau.

### Dans cette section

Navigation .....	<a href="#">318</a>
Configuration de la tâche Protection du trafic.....	<a href="#">319</a>
Configuration de la protection contre les applications malveillantes sur Internet.....	<a href="#">324</a>
Configuration de la protection contre les menaces email.....	<a href="#">327</a>
Configuration du traitement des adresses et des sites Internet .....	<a href="#">327</a>
Configuration du Contrôle Internet.....	<a href="#">329</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Accès aux paramètres de la stratégie pour la tâche Protection du trafic .....	<a href="#">318</a>
Accès à la liste des règles de la Protection du trafic .....	<a href="#">319</a>

## Accès aux paramètres de la stratégie pour la tâche Protection du trafic

► *Pour accéder aux paramètres de la tâche Contrôle du lancement des applications via une stratégie de*

*Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.

Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel du serveur**.

5. Cliquez sur le bouton **Configuration** dans la sous-section **Protection du trafic**.  
La fenêtre **Protection du trafic** s'ouvre.
6. Configurez la stratégie en fonction des besoins.

## Accès à la liste des règles de la Protection du trafic

► *Pour accéder à la liste des règles du Contrôle du lancement des applications via Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel du serveur**.
6. Cliquez sur le bouton **Liste des règles** dans la sous-section **Protection du trafic**.

La fenêtre **Règles de contrôle Internet** s'ouvre.

Configurez la liste des règles en fonction des besoins.

## Configuration de la tâche Protection du trafic

► *Pour configurer la tâche Protection du trafic :*

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Mode de tâche**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section "Configuration du mode de fonctionnement de la tâche" à la page [320](#)).
3. Sous l'onglet **Traitement des adresses et des sites Internet**, configurez l'analyse antivirus et anti-phishing des adresses Internet (cf. section "Configuration du traitement des adresses et des sites Internet" à la page [327](#)).
4. Sous l'onglet **Protection contre les applications malveillantes**, configurez l'analyse heuristique et le niveau de sécurité (cf. section "Configuration de la protection contre les applications malveillantes sur

Internet" à la page [324](#)).

5. Sous l'onglet **Administration des tâches**, configurez les paramètres de lancement de la tâche selon une planification (cf. section "Programmation des tâches" à la page [138](#)).
6. Cliquez sur le bouton **OK**.

La configuration de la tâche est enregistrée.

## Dans cette section

Configuration du mode de fonctionnement de la tâche .....	<a href="#">320</a>
Configuration du mode Intercepteur de pilote .....	<a href="#">321</a>
Configuration du mode Redirection .....	<a href="#">323</a>

## Configuration du mode de fonctionnement de la tâche

### ► Pour configurer le mode de fonctionnement d'une tâche :

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Général**, sélectionnez un des modes disponibles dans la liste déroulante **Mode de tâche** :
  - **Intercepteur de pilote** (cf. section "**Configuration du mode Intercepteur de pilote**" à la page [321](#))
  - **Redirection** (cf. section "**Configuration du mode Redirection**" à la page [323](#))
  - **Proxy externe**
3. Définissez les paramètres de connexion du service ICAP (requis pour les trois modes) :
  - **Numéro de port réseau**

Le numéro de port du service ICAP pour Kaspersky Security for Windows Server.
  - **Identification du service**

Identifiant qui fait partie du paramètre RESPMOD URI du protocole ICAP (cf. document RFC 3507). RESPMOD URI désigne l'adresse du serveur ICAP antivirus installé pour le stockage réseau.

Par exemple, si l'adresse IP du serveur protégé est 192.168.10.10, que le numéro de port est 1345 et que l'identification du service ICAP est webscan, l'adresse RESPMOD URI correspondante est : icap://192.168.10.10/webscan:1345

Redémarrez la tâche pour appliquer les paramètres de connexion du service ICAP.

4. Configurez le mode de fonctionnement de tâche sélectionné.

Aucune configuration complémentaire n'est requise pour le mode **Proxy externe**. La configuration est réalisée sur le serveur proxy externe.

5. Cliquez sur le bouton **OK**.  
La configuration est enregistrée.

## Configuration du mode Intercepteur de pilote

► Pour configurer le mode Intercepteur de pilote, procédez comme suit :

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Général**, sélectionnez le mode de tâche **Intercepteur de pilote**.
3. Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :

- **Vérifier les connexions sécurisées via le protocole HTTPS.**

Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
  - **HNAS 1.0**
  - **HNAS 1.1**
  - **HNAS 1.2**

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

- **Ne pas faire confiance aux serveurs Internet dotés d'un certificat non valide.**

La case peut être cochée uniquement si la case **Vérifier les connexions sécurisées via le protocole HTTPS** est cochée.

Si la case est cochée, une page Internet dotée d'un certificat non valide est bloquée (le certificat a expiré, erreur de vérification de la signature, certificat révoqué, etc.).

- **Port de sécurité.**

Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Vérifier les connexions sécurisées via le protocole HTTPS**.

4. Pour ajouter ou exclure des ports depuis la zone d'interception, cliquez sur le bouton **Configurer la zone d'interception**.



La fenêtre **Zone d'interception** s'ouvre.

5. Sélectionnez une des options suivantes sous l'onglet **Intercepter les ports** :
  - **Tout intercepter**
  - **Intercepter les ports indiqués** :
    - a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.
    - b. Cliquez sur **Ajouter**.

Le port est inclus dans la zone d'interception.

Par défaut, Kaspersky Security for Windows Server intercepte le trafic transféré via les ports suivants : 80, 8080, 3128, 443.

6. Pour désigner les ports que vous souhaitez exclure de la zone d'interception sous l'onglet **Exclure les ports** :
  - a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.
  - b. Cliquez sur **Ajouter**.

Le port est exclu de la zone.

Par défaut Kaspersky Security for Windows Server exclut les ports utilisés par d'autres applications et risque de générer des problèmes lors de la tentative de lecture des données transférées par connexion chiffrée : 3389, 1723, 13291.

7. Pour exclure des adresses IP de la zone d'interception sous l'onglet **Exclure les adresses IP**, procédez comme suit :
  - a. Saisissez l'adresse IP au format IPv4 (format court ou en définissant une adresse avec un masque de sous-réseau).
  - b. Cliquez sur **Ajouter**.
  - c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
8. Pour exclure le processus ou le fichier exécutable qui requiert un échange de trafic sous l'onglet **Exclure les processus** :
  - a. Cochez la case **Appliquer les exclusions pour les processus**.
  - b. Pour exclure un fichier :
    1. Cliquez sur le bouton **Fichiers exécutables**.

La fenêtre standard **Ouvrir** s'ouvre.
    2. Sélectionnez le fichier exécutable que vous souhaitez exclure, puis cliquez sur **Ouvrir**.
9. Dans la fenêtre **Zone d'interception**, cliquez sur le bouton **OK**.
10. Dans la fenêtre **Protection du trafic**, cliquez sur le bouton **OK**.

La configuration du mode de tâche est enregistrée.

## Configuration du mode Redirection

► Pour configurer le mode Redirection, procédez comme suit :

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Général**, sélectionnez le mode de tâche **Redirection**.
3. Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :

- **Vérifier les connexions sécurisées via le protocole HTTPS.**

Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :

- **HNAS 1.0**
- **HNAS 1.1**
- **HNAS 1.2**

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

- **Renvoyer le trafic vers le serveur proxy après l'analyse.**

Si la case est cochée, Kaspersky Security for Windows Server redirige le trafic qui a déjà été analysé vers un proxy externe, par exemple un serveur proxy d'entreprise qui est utilisé au sein du réseau de l'entreprise.

Si la case est décochée, le trafic est envoyé directement à un proxy interne.

- **Adresse du serveur proxy.**

L'adresse du serveur proxy interne intervient dans la redirection. Saisissez l'adresse au format IPv4.

- **Port.**

Le numéro de port du proxy Interne.

- **Port de sécurité.**

Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Vérifier les connexions sécurisées via le protocole HTTPS**.

Dans le mode **Redirection**, le système d'exploitation doit être configuré de telle sorte que le trafic chiffré est transmis via le port indiqué par Kaspersky Security for Windows Server.

4. Cliquez sur le bouton **OK**.

La configuration du mode de tâche est enregistrée.

## Configuration de la protection contre les applications malveillantes sur Internet

Les paramètres de protection suivants affectent également tout le trafic entrant. Cependant, les actions sélectionnées sur les objets infectés et les autres objets détectés sont effectuées uniquement pour les pièces jointes de l'email.

- *Pour configurer l'analyse heuristique en vue de détecter les virus et autres menaces contre la sécurité informatique transmises via le trafic Internet :*

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Protection contre les applications malveillantes** :
  - Cochez la case **Utiliser l'analyse heuristique**.
  - Définissez le niveau requis d'analyse heuristique pour la recherche d'applications malveillantes.
  - Sélectionnez le niveau de sécurité (cf. section "Paramètres de niveau de protection prédéfini" à la page [316](#)) dans le menu déroulant :
    - **Recommandé**
    - **Protection maximale**
    - **Performance maximale**
    - **Personnalisé**
3. Ouvrez l'onglet **Général** en cliquant sur **Configuration**, puis, dans la section **Protection d'objet**, indiquez les objets que vous souhaitez inclure à la zone d'analyse :
  - **Tous les objets**

Kaspersky Security for Windows Server analyse tous les objets.
  - **Objets analysés en fonction du format**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.
  - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- a. Cliquez sur le bouton **Modifier** pour modifier la liste des extensions.
- b. Indiquez une extension dans la fenêtre qui s'ouvre.
- c. Cliquez sur **Ajouter**.

Cliquez sur le bouton **Par défaut** pour remplir la liste à l'aide de la liste prédéfinie des extensions exclues.

4. Dans la section **Protection d'objet composé**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

- **Archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Objets OLE intégrés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés

au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

5. Sous l'onglet **Actions**, sélectionnez l'action à exécuter sur les objets infectés et sur les autres objets détectés :

- **Interdire**

Kaspersky Security for Windows Server interdit le chargement de toute page Internet sur laquelle du contenu malveillant a été détecté. La raison de l'interdiction est affichée au lieu de la page.

Kaspersky Security for Windows Server supprime définitivement les pièces jointes infectées des messages électroniques. Dans ce cas, les événements sur les menaces découvertes sont enregistrées dans le journal d'exécution de la tâche Protection du trafic.

- **Autoriser**

Kaspersky Security for Windows Server n'interdit pas le chargement de la page sollicitée, mais consigne dans le journal la détection du contenu malveillant.

Kaspersky Security for Windows Server ne supprime pas les pièces jointes infectées des messages électroniques. Dans ce cas, les événements sur les menaces découvertes sont enregistrées dans le journal d'exécution de la tâche Protection du trafic.

6. Sous l'onglet **Optimisation**, configurez les paramètres suivants :

- Dans la section **Exclusions**, cochez ou décochez la case **Ne pas détecter**. Pour configurer la liste des objets à exclure :

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus <https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- a. Cliquez sur le bouton **Modifier**.
  - b. Dans la fenêtre qui s'ouvre, indiquez le nom de l'objet ou le masque.
  - c. Cliquez sur **Ajouter**.
- Dans la section **Paramètres avancés**, limitez l'intervalle d'analyse et la taille de l'objet :
    - **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Kaspersky Security for Windows Server ignore lors de la recherche de virus les objets dont la taille est supérieure à la valeur indiquée.

La valeur est égale par défaut à 20 Mo.

1. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de protection contre les applications malveillantes**.

La configuration du niveau de sécurité est enregistrée.

## Configuration de la protection contre les menaces email

Pour utiliser la protection contre les menaces email, le Plug-in Microsoft Outlook doit être installé et le serveur protégé, configuré (cf. section "Protection contre les menaces email" à la page [311](#)).

► *Pour activer la protection contre les menaces email :*

1. Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Protection contre les menaces email**, cochez la case **Activer la protection contre les menaces email**.

Si la case est cochée, Kaspersky Security for Windows Server utilise le Plug-in Kaspersky Security pour Microsoft Outlook afin de procéder à une analyse antiphishing et antivirus de tout le courrier entrant et sortant.

Si la case est décochée, le courrier n'est pas analysé.

Cette case est cochée par défaut.

Si vous activez ou désactivez la protection contre les menaces email, les modifications entrent en vigueur après un bref délai (5 minutes) ou immédiatement après le redémarrage de Microsoft Outlook.

3. Cliquez sur le bouton **OK**.

Les modifications sont enregistrées.

## Configuration du traitement des adresses et des sites Internet

► *Pour rechercher la présence éventuelle de menaces de phishing sur des ressources Internet et identifier les adresses Internet considérées comme malveillantes par les bases antivirus et la réputation des adresses Internet de KSN :*

1. **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
2. Sous l'onglet **Général**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section

"Configuration du mode de fonctionnement de la tâche" à la page [320](#)).

3. Sous l'onglet **Traitement des adresses et des sites Internet** :

- Décochez ou cochez la case **Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes**.

Si la case est cochée, Kaspersky Security for Windows Server analyse chaque adresse Internet selon les signatures.

Si la case est décochée, les bases antivirus n'interviennent pas dans l'analyse des adresses Internet.

Cette case est cochée par défaut.

- Décochez ou cochez la case **Analyser les pages Internet à l'aide de la base de données anti-phishing**.

Si la case est cochée, Kaspersky Security for Windows Server analyse chaque adresse Internet à l'aide des bases anti-phishing. L'analyse anti-phishing repose sur l'analyse heuristique.

Si la case est décochée, Kaspersky Security for Windows Server ne détecte pas les attaques de phishing.

Cette case est cochée par défaut.

Sachez que quand vous configurez l'analyse anti-phishing des adresses Internet, l'anti-phishing est appliqué automatiquement aux emails.

- Cochez ou décochez la case **Utiliser la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

- Cochez ou décochez la case **Utiliser KSN pour la protection**.

Cette case active ou désactive l'utilisation des services KSN.

Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs.

Si la case est décochée, la tâche n'utilise pas les services du KSN.

Cette case est cochée par défaut.

La réputation KSN d'une adresse Internet est disponible uniquement si toutes les conditions suivantes sont remplies :

- La case **Utiliser KSN pour la protection** a été cochée dans les paramètres de la Protection du trafic
- La Déclaration de KSN a été acceptée.
- La case **Envoyer les données relatives aux URL sollicitées** (cf. section "**Configuration de la**

tâche **Utilisation du KSN via le plug-in d'administration**" à la page [298](#)) est cochée.

- La tâche Utilisation du KSN est lancée.

4. Cliquez sur le bouton **OK**.

La configuration du traitement des adresses et des sites Internet est enregistrée.

## Configuration du Contrôle Internet

Gérez les paramètres de traitement des adresses et des sites Internet, les règles et l'analyse des certificats et le contrôle Internet basé sur les catégories.

### Dans cette section

Configuration de l'analyse des certificats .....	<a href="#">329</a>
Configuration du Contrôle Internet basé sur les catégories .....	<a href="#">331</a>
Ajout de règles en fonction des adresses Internet .....	<a href="#">332</a>

## Configuration de l'analyse des certificats

Kaspersky Security for Windows Server permet d'analyser les certificats et d'interdire les ressources Internet dont les certificats sont non valides ou expirés. Pour configurer l'analyse des certificats, il faut réaliser les opérations suivantes :

- Configurez la tâche Protection du trafic (cf. section "Sélection et configuration du mode de " à la page [329](#)).
- Ajoutez et appliquez des Règles pour les certificats (cf. section "Ajout de règles pour les certificats" à la page [330](#)).

Les règles pour les certificats peuvent uniquement être utilisées dans les modes **Intercepteur de pilote** ou **Redirection**. Kaspersky Security for Windows Server crée uniquement des règles d'interdiction pour les certificats.

### Sélection et configuration du mode de tâche

► *Pour sélectionner et configurer le mode d'utilisation des certificats :*

- Ouvrez la fenêtre **Protection du trafic** (cf. section "Accès aux paramètres de la stratégie pour la tâche Protection du trafic" à la page [318](#)).
- Sous l'onglet **Général**, sélectionnez un des modes qui prend en charge l'analyse de certificats dans la liste déroulante **Mode de tâche** :
  - **Intercepteur de pilote** (cf. section "**Configuration du mode Intercepteur de pilote**" à la page [321](#))
  - **Redirection** (cf. section "**Configuration du mode Redirection**" à la page [323](#))
- Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :
  - **Vérifier les connexions sécurisées via le protocole HTTPS**.

Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la



recherche de menaces.

Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
  - **HNAS 1.0**
  - **HNAS 1.1**
  - **HNAS 1.2**

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

4. Cliquez sur le bouton **OK**.

La configuration de la tâche est enregistrée.

## Ajout de règles pour les certificats

Les certificats peuvent uniquement être utilisés dans les modes **Intercepteur de pilote** ou **Redirection**. Kaspersky Security for Windows Server crée uniquement des règles d'interdiction pour les certificats.

► *Pour ajouter ou configurer une règle pour un certificat :*

1. Ouvrez la fenêtre **Règles de contrôle Internet** (cf. section "Accès à la liste des règles de protection du trafic" à la page [319](#)).
2. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles basées sur l'URL** pour appliquer les règles.

Si la case est cochée, Kaspersky Security for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

Si la case est décochée, les certificats ne sont pas analysés par l'application.

Cette case est cochée par défaut.

3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
4. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon le certificat**.
5. Dans la fenêtre **Règle selon le certificat** qui s'ouvre :
  - a. Saisissez le nom de la règle.
  - b. Cochez la case **Appliquer la règle**.
  - c. Sélectionnez le **Type d'opérateur** : **Utiliser les symboles de masques** ou **Utiliser les expressions régulières**.
  - d. Définissez le masque ou l'expression dans le champ **Opérateur**.
  - e. Cliquez sur le bouton **OK**.

6. Pour modifier une règle, sélectionnez la règle en question dans la liste et cliquez sur **Modifier**.
7. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles de Contrôle Internet**.

Les nouvelles règles sont appliquées.

## Configuration du Contrôle Internet basé sur les catégories

► *Pour ajouter ou modifier une règle de la Protection du trafic basée sur les catégories :*

1. Ouvrez la fenêtre **Règles de contrôle Internet** (cf. section "**Ouverture de la fenêtre des règles de protection du trafic**" à la page [319](#)).
2. Ouvrez l'onglet **Catégories**.
3. Cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.

Si la case est cochée, Kaspersky Security for Windows Server définit les catégories des ressources Internet et interdit celles qui appartiennent aux catégories sélectionnées.

Si la case est décochée, Kaspersky Security for Windows Server ne définit pas les catégories.

Cette case est décochée par défaut.

Les paramètres du contrôle de catégorie deviennent disponibles.

4. Cochez ou décochez les cases suivantes :
  - **Autoriser l'accès si la page Internet ne peut pas être classée dans une catégorie.**
  - **Autoriser l'accès aux ressources Internet légitimes qui peuvent servir à nuire au serveur.**
  - **Autoriser l'accès aux publicités légitimes.**
5. Dans la liste des catégories disponibles (cf. section "Liste des catégories" à la page [312](#)) :
  - Cochez la case correspondante pour autoriser une catégorie.  
La colonne **Type de règle** passe à l'état **Autorisé**.
  - Décochez la case correspondante pour interdire une catégorie.  
La colonne **Type de règle** passe à l'état **Interdit**.

La liste des catégories est prédéfinie et ne peut être modifiée (il est impossible d'ajouter ou de supprimer des catégories).

6. Cliquez sur le bouton **OK**.

La configuration des règles est enregistrée.

### Utilisation du masque not-a-virus

► *Pour utiliser le masque `not-a-virus` dans le cadre de l'analyse d'une catégorie :*

1. Dans la Console d'administration de Kaspersky Security Center, ouvrez les paramètres de la tâche Utilisation du KSN (cf. section "Configuration de la tâche Utilisation du KSN via le plug-in d'administration" à

la page [298](#)).

2. Cochez la case **Envoyer les données relatives aux URL sollicitées**.
3. Lancez tâche Utilisation du KSN.
4. Dans la fenêtre de configuration de la Protection du trafic (cf. section "Configuration de la tâche Protection du trafic" à la page [319](#)), cochez la case **Utiliser KSN pour la protection**.
5. Dans la fenêtre **Règles de Contrôle Internet**, sous l'onglet **Catégories**, cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.
6. Dans la liste des catégories, sélectionnez les catégories pour lesquelles vous souhaitez appliquer le masque `not-a-virus`.

Les objets des catégories sélectionnées qui correspondent au masque ne seront pas détectés par la tâche Protection du trafic.

L'utilisation du masque `not-a-virus` est configurée dans les paramètres de la Zone de confiance (cf. section "Application du masque not-a-virus" à la page [527](#)).

## Ajout de règles en fonction des adresses Internet

Vous pouvez ajouter une règle en fonction d'une adresse Internet pour autoriser ou interdire une adresse Internet en particulier. Ces règles ont une priorité supérieure à celle de n'importe quelle autre conclusion.

### ► Pour créer une règle sur la base d'une adresse Internet :

1. Ouvrez la fenêtre **Règles de contrôle Internet** (cf. section "Accès à la liste des règles de protection du trafic" à la page [319](#)).
2. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles basées sur l'URL** pour appliquer les règles.

Si la case est cochée, Kaspersky Security for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

Si la case est décochée, les certificats ne sont pas analysés par l'application.

Cette case est cochée par défaut.

3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
4. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon l'adresse Internet**.
5. Dans la fenêtre **Règle selon l'adresse Internet** qui s'ouvre :
  - a. Saisissez le nom de la règle.
  - b. Sélectionnez le **Type de règle** : **Interdit** ou **Autorisé**.
  - c. Cochez la case **Appliquer la règle**.
  - d. Indiquez l'URL dans le champ **Adresse Internet**.
  - e. Cliquez sur le bouton **OK**.
6. Pour modifier une règle, sélectionnez la règle en question dans la liste et cliquez sur **Modifier**.
7. Dans la fenêtre **Règles de contrôle Internet**, cliquez sur le bouton **OK**.

Les nouvelles règles sont appliquées.

## Administration de la protection du trafic via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un serveur local.

### Dans cette section

Navigation .....	<a href="#">333</a>
Configuration de la tâche Protection du trafic.....	<a href="#">334</a>
Configuration de la protection contre les applications malveillantes sur Internet.....	<a href="#">338</a>
Configuration de la protection contre les menaces email.....	<a href="#">341</a>
Configuration du traitement des adresses et des sites Internet .....	<a href="#">342</a>
Configuration du Contrôle Internet.....	<a href="#">343</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Accès aux paramètres de la tâche Protection du trafic .....	<a href="#">333</a>
Ouverture de la fenêtre des règles de la protection du trafic .....	<a href="#">334</a>

## Accès aux paramètres de la tâche Protection du trafic

► *Pour accéder aux paramètres généraux de la tâche Protection du trafic via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection du trafic**.
3. Dans le panneau de détails du nœud **Protection du trafic**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

## Ouverture de la fenêtre des règles de la protection du trafic

► *Pour ouvrir la liste des règles de protection du trafic via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection du trafic**.
3. Dans le panneau de détails du nœud **Protection du trafic**, cliquez sur le lien **Règles de Contrôle Internet**.  
La fenêtre **Règles de Contrôle Internet** s'ouvre.  
Configurez la liste des règles en fonction des besoins.

## Configuration de la tâche Protection du trafic

► *Pour configurer la tâche Protection du trafic :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Général**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section "Configuration du mode de fonctionnement de la tâche" à la page [334](#)).
3. Sous l'onglet **Traitement des adresses et des sites Internet**, configurez l'analyse antivirus et anti-phishing des adresses Internet (cf. section "Configuration du mode Intercepteur de pilote" à la page [335](#)).
4. Sous l'onglet **Protection contre les applications malveillantes**, configurez l'analyse heuristique et le niveau de sécurité (cf. section "Configuration de la protection contre les applications malveillantes sur Internet" à la page [338](#)).
5. Sous les onglets **Planification** et **Avancé**, lancez la tâche selon une planification (cf. section "Programmation des tâches" à la page [138](#)).
6. Cliquez sur le bouton **OK** pour enregistrer les modifications.

### Dans cette section

Configuration du mode de fonctionnement de la tâche .....	<a href="#">334</a>
Configuration du mode Intercepteur de pilote .....	<a href="#">335</a>
Configuration du mode Redirection .....	<a href="#">337</a>

## Configuration du mode de fonctionnement de la tâche

► *Pour configurer le mode de fonctionnement d'une tâche :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Général**, sélectionnez un des modes disponibles dans la liste déroulante **Mode de tâche** :

- **Intercepteur de pilote**
  - **Redirection**
  - **Proxy externe**
3. Définissez les **Paramètres de connexion au service ICAP** (requis pour les trois modes) :

- **Numéro de port réseau**

Le numéro de port du service ICAP pour Kaspersky Security for Windows Server.

- **Identification du service**

Identifiant qui fait partie du paramètre RESPMOD URI du protocole ICAP (cf. document RFC 3507). RESPMOD URI désigne l'adresse du serveur ICAP antivirus installé pour le stockage réseau.

Par exemple, si l'adresse IP du serveur protégé est 192.168.10.10, que le numéro de port est 1345 et que l'identification du service ICAP est webscan, l'adresse RESPMOD URI correspondante est : icap://192.168.10.10/webscan:1345

Redémarrez la tâche pour appliquer les paramètres de connexion du service ICAP.

4. Configurez le mode de fonctionnement de tâche sélectionné.

Aucune configuration complémentaire n'est requise pour le mode **Proxy externe**. La configuration est réalisée sur le serveur proxy externe.

5. Cliquez sur le bouton **OK**.

La configuration est enregistrée.

## Configuration du mode Intercepteur de pilote

► Pour configurer le mode Intercepteur de pilote, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Général**, sélectionnez le mode de tâche **Intercepteur de pilote**.
3. Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :

- **Vérifier les connexions sécurisées via le protocole HTTPS.**

Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :

- HNAS 1.0
- HNAS 1.1
- HNAS 1.2

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

- **Ne pas faire confiance aux serveurs Internet dotés d'un certificat non valide.**

La case peut être cochée uniquement si la case **Vérifier les connexions sécurisées via le protocole HTTPS** est cochée.

Si la case est cochée, une page Internet dotée d'un certificat non valide est bloquée (le certificat a expiré, erreur de vérification de la signature, certificat révoqué, etc.).

- **Port de sécurité.**

Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Vérifier les connexions sécurisées via le protocole HTTPS**.

4. Pour ajouter ou exclure des ports depuis la zone d'interception, cliquez sur le bouton **Configurer la zone d'interception**.

La fenêtre **Zone d'interception** s'ouvre.

5. Sélectionnez une des options suivantes sous l'onglet **Intercepter les ports** :

- **Tout intercepter**

- **Intercepter les ports indiqués :**

- a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.
- b. Cliquez sur **Ajouter**.

Le port est inclus dans la zone d'interception.

Par défaut, Kaspersky Security for Windows Server intercepte le trafic transféré via les ports suivants : 80, 8080, 3128, 443.

6. Pour désigner les ports que vous souhaitez exclure de la zone d'interception sous l'onglet **Exclure les ports** :

- a. Saisissez le numéro du port dans le champ textuel. Si vous souhaitez saisir plusieurs ports, séparez-les par un point-virgule.
- b. Cliquez sur **Ajouter**.

Le port est exclu de la zone.

Par défaut Kaspersky Security for Windows Server exclut les ports utilisés par d'autres applications et risque de générer des problèmes lors de la tentative de lecture des données transférées par connexion chiffrée : 3389, 1723, 13291.

7. Pour exclure des adresses IP de la zone d'interception sous l'onglet **Exclure les adresses IP**, procédez comme suit :
    - a. Saisissez l'adresse IP au format IPv4 (format court ou en définissant une adresse avec un masque de sous-réseau).
    - b. Cliquez sur **Ajouter**.
    - c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
  8. Pour exclure le processus ou le fichier exécutable qui requiert un échange de trafic sous l'onglet **Exclure les processus** :
    - a. Cochez la case **Appliquer les exclusions pour les processus**.
    - b. Pour exclure un fichier :
      1. Cliquez sur le bouton **Fichiers exécutables**.  
La fenêtre standard **Ouvrir** s'ouvre.
      2. Sélectionnez le fichier exécutable que vous souhaitez exclure, puis cliquez sur **Ouvrir**.
  9. Dans la fenêtre **Zone d'interception**, cliquez sur le bouton **OK**.
  10. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.
- La configuration du mode de tâche est enregistrée.

## Configuration du mode Redirection

► *Pour configurer le mode Redirection, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Général**, sélectionnez le mode de tâche **Redirection**.
3. Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :
  - **Vérifier les connexions sécurisées via le protocole HTTPS.**
    - Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.
    - Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.
    - Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
  - **HNAS 1.0**
  - **HNAS 1.1**



- **HNAS 1.2**

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

- **Port de sécurité.**

Indiquez le numéro de port utilisé pour rediriger le trafic depuis le navigateur ou le pilote réseau vers Kaspersky Security for Windows Server afin de détecter les menaces Internet. Il est déconseillé de modifier le port par défaut. Le numéro de port ne doit coïncider avec aucun des ports ouverts pour le service ICAP. Si vous utilisez le mode de tâche **Redirection**, les ports qui sont déjà utilisés figurent dans le champ **Vérifier les connexions sécurisées via le protocole HTTPS**.

- **Rediriger le trafic vers un proxy externe après la vérification.**

Si la case est cochée, Kaspersky Security for Windows Server redirige le trafic qui a déjà été analysé vers un proxy externe, par exemple un serveur proxy d'entreprise qui est utilisé au sein du réseau de l'entreprise.

Si la case est décochée, le trafic est envoyé directement à un proxy interne.

- **Adresse du serveur proxy.**

L'adresse du serveur proxy interne intervient dans la redirection. Saisissez l'adresse au format IPv4.

- **Port.**

Le numéro de port du proxy Interne.

Dans le mode **Redirection**, le système d'exploitation doit être configuré de telle sorte que le trafic chiffré est transmis via le port indiqué par Kaspersky Security for Windows Server.

4. Cliquez sur le bouton **OK**.

La configuration du mode de tâche est enregistrée.

## Configuration de la protection contre les applications malveillantes sur Internet

Les paramètres de protection suivants affectent également tout le trafic entrant. Cependant, les actions sélectionnées sur les objets infectés et les autres objets détectés sont effectuées uniquement pour les pièces jointes de l'email.

► *Pour configurer l'analyse heuristique en vue de détecter les virus et autres menaces contre la sécurité informatique transmises via le trafic Internet :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du**

trafic" à la page [333](#)).

2. Sous l'onglet **Protection contre les applications malveillantes** :

- Cochez la case **Utiliser l'analyse heuristique**.
- Définissez le niveau requis d'analyse heuristique pour la recherche d'applications malveillantes.
- Sélectionnez le niveau de protection (cf. section "Paramètres de niveau de protection prédéfini" à la page [316](#)) dans le menu déroulant :
  - **Recommandé**
  - **Protection maximale**
  - **Performance maximale**
  - **Personnalisé**

3. L'onglet **Description** de la partie inférieure permet de consulter les paramètres du niveau de protection sélectionné.

4. Ouvrez l'onglet **Général**, puis, dans la section **Protection des objets**, indiquez les objets que vous souhaitez inclure dans la zone d'analyse :

- **Tous les objets**

Kaspersky Security for Windows Server analyse tous les objets.

- **Objets analysés en fonction du format**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- a. Cliquez sur le bouton **Modifier** pour modifier la liste des extensions.
- b. Indiquez une extension dans la fenêtre qui s'ouvre.
- c. Cliquez sur **Ajouter**.

Cliquez sur le bouton **Par défaut** pour remplir la liste à l'aide de la liste prédéfinie des extensions exclues.

5. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

- **Archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Objets OLE intégrés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

6. Sous l'onglet **Actions**, sélectionnez l'action à exécuter sur les objets infectés et sur les autres objets détectés :

- **Interdire**

Kaspersky Security for Windows Server interdit le chargement de toute page Internet sur laquelle du contenu malveillant a été détecté. La raison de l'interdiction est affichée au lieu de la page.

Kaspersky Security for Windows Server supprime définitivement les pièces jointes infectées des messages électroniques. Dans ce cas, les événements sur les menaces découvertes sont enregistrées dans le journal d'exécution de la tâche Protection du trafic.

- **Autoriser**

Kaspersky Security for Windows Server n'interdit pas le chargement de la page sollicitée, mais consigne dans le journal la détection du contenu malveillant.

Kaspersky Security for Windows Server ne supprime pas les pièces jointes infectées des

messages électroniques. Dans ce cas, les événements sur les menaces découvertes sont enregistrées dans le journal d'exécution de la tâche Protection du trafic.

7. Sous l'onglet **Optimisation**, configurez les paramètres suivants :

- Dans la section **Exclusions**, cochez ou décochez la case **Ne pas détecter**. Pour configurer la liste des objets à exclure :

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus <https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- Cliquez sur le bouton **Modifier**.
  - Dans la fenêtre qui s'ouvre, indiquez le nom de l'objet ou le masque.
  - Cliquez sur **Ajouter**.
- Dans la section **Paramètres avancés**, limitez l'intervalle d'analyse et la taille de l'objet :

- **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Kaspersky Security for Windows Server ignore lors de la recherche de virus les objets dont la taille est supérieure à la valeur indiquée.

La valeur est égale par défaut à 20 Mo.

1. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

La configuration du niveau de protection est enregistrée.

## Configuration de la protection contre les menaces email

► *Pour activer la protection contre les menaces email :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Protection contre les menaces email**, cochez la case **Activer la protection contre les menaces email**.

Si la case est cochée, Kaspersky Security for Windows Server utilise le Plug-in Kaspersky

Security pour Microsoft Outlook afin de procéder à une analyse antiphishing et antivirus de tout le courrier entrant et sortant.

Si la case est décochée, le courrier n'est pas analysé.

Cette case est cochée par défaut.

Si vous activez ou désactivez la protection contre les menaces email, les modifications entrent en vigueur après un bref délai (5 minutes) ou immédiatement après le redémarrage de Microsoft Outlook.

3. Cliquez sur le bouton **OK**.

Les modifications sont enregistrées.

## Configuration du traitement des adresses et des sites Internet

Pour rechercher la présence éventuelle de menaces de phishing sur des ressources Internet et identifier les adresses Internet considérées comme malveillantes par les bases antivirus et la réputation des adresses Internet de KSN :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Dans la section **Mode de tâche** de l'onglet **Général**, sélectionnez et configurez le mode de fonctionnement de la tâche (cf. section "Configuration du mode de fonctionnement de la tâche" à la page [334](#)).
3. Sous l'onglet **Traitement des adresses et des sites Internet** :

- Décochez ou cochez la case **Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes**.

Si la case est cochée, Kaspersky Security for Windows Server analyse chaque adresse Internet selon les signatures.

Si la case est décochée, les bases antivirus n'interviennent pas dans l'analyse des adresses Internet.

Cette case est cochée par défaut.

- Décochez ou cochez la case **Analyser les pages Internet à l'aide de la base de données anti-phishing**.

Si la case est cochée, Kaspersky Security for Windows Server analyse chaque adresse Internet à l'aide des bases anti-phishing. L'analyse anti-phishing repose sur l'analyse heuristique.

Si la case est décochée, Kaspersky Security for Windows Server ne détecte pas les attaques de phishing.

Cette case est cochée par défaut.

Sachez que quand vous configurez l'analyse anti-phishing des adresses Internet, l'anti-phishing est appliqué automatiquement aux emails.

- Cochez ou décochez la case **Utiliser la zone de confiance**.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur

les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

- Cochez ou décochez la case **Utiliser KSN pour la protection**.

Cette case active ou désactive l'utilisation des services KSN.

Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs.

Si la case est décochée, la tâche n'utilise pas les services du KSN.

Cette case est cochée par défaut.

La réputation KSN d'une adresse Internet est disponible uniquement si toutes les conditions suivantes sont remplies :

- La case **Utiliser KSN pour la protection** a été cochée dans les paramètres de la Protection du trafic
- La Déclaration de KSN a été acceptée.
- La case **Envoyer des données relatives aux URL analysées** (cf. section "**Configuration de la tâche Utilisation du KSN via la Console de l'application**" à la page [302](#)) est cochée.
- La tâche Utilisation du KSN est lancée.

4. Cliquez sur le bouton **OK**.

La configuration du traitement des adresses et des sites Internet est enregistrée.

## Configuration du Contrôle Internet

Gérez les paramètres de traitement des adresses et des sites Internet, les règles et l'analyse des certificats et le contrôle Internet basé sur les catégories.

### Dans cette section

Configuration de l'analyse des certificats .....	<a href="#">343</a>
Configuration du Contrôle Internet basé sur les catégories .....	<a href="#">345</a>
Ajout de règles en fonction des adresses Internet .....	<a href="#">346</a>

## Configuration de l'analyse des certificats

Kaspersky Security for Windows Server permet d'analyser les certificats et d'interdire les ressources Internet dont les certificats sont non valides ou expirés. Pour configurer l'analyse des certificats, il faut réaliser les opérations suivantes :

- a. Configurez la tâche Protection du trafic (cf. section "Sélection et configuration du mode de " à la page [344](#)).

- b. Ajoutez et appliquez des Règles pour les certificats (cf. section "Ajout de règles pour les certificats" à la page [344](#)).

Les règles pour les certificats peuvent uniquement être utilisées dans les modes **Intercepteur de pilote** ou **Redirection**. Kaspersky Security for Windows Server crée uniquement des règles d'interdiction pour les certificats.

## Sélection et configuration du mode de tâche

Pour sélectionner et configurer le mode d'utilisation des certificats :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Protection du trafic**" à la page [333](#)).
2. Sous l'onglet **Général**, sélectionnez un des modes qui prend en charge l'analyse de certificats dans la liste déroulante **Mode de tâche** :
  - **Intercepteur de pilote** (cf. section "**Configuration du mode Intercepteur de pilote**" à la page [335](#))
  - **Redirection**
3. Dans le groupe **Paramètres du mode de tâche**, configurez les paramètres suivants :

- **Vérifier les connexions sécurisées via le protocole HTTPS.**

Si la case est cochée, le trafic HTTPS chiffré est intercepté et décompressé et soumis à la recherche de menaces.

Si la case n'est pas cochée, le trafic HTTPS chiffré n'est pas décompressé.

Cette case est cochée par défaut.

L'analyse est disponible uniquement si le port HTTPS est ouvert.

- Sélectionnez la version du protocole de chiffrement que vous souhaitez utiliser :
  - **HNAS 1.0**
  - **HNAS 1.1**
  - **HNAS 1.2**

Toutes les versions sont sélectionnées par défaut. Dans ce cas, l'option **TLS 1.0** ne peut pas être désactivée.

4. Cliquez sur le bouton **OK**.

La configuration de la tâche est enregistrée.

## Ajout de règles pour les certificats

Les certificats peuvent uniquement être utilisés dans les modes **Intercepteur de pilote** ou **Redirection**. Par défaut, Kaspersky Security 10.1.1 crée uniquement des règles d'interdiction pour les certificats.

► *Pour ajouter ou configurer une règle pour un certificat :*

1. Ouvrez la fenêtre **Règles de Contrôle Internet** (cf. section "Ouverture de la fenêtre des règles de

protection du trafic" à la page [334](#)).

2. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles basées sur l'URL** pour appliquer les règles.

Si la case est cochée, Kaspersky Security for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

Si la case est décochée, les certificats ne sont pas analysés par l'application.

Cette case est cochée par défaut.

3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
4. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon le certificat**.
5. Dans la fenêtre **Règle selon le certificat** qui s'ouvre :
  - a. Saisissez le nom de la règle.
  - b. Cochez la case **Appliquer la règle**.
  - c. Sélectionnez le **Type d'opérateur** : **Utiliser les symboles de masque** ou **Utiliser les expressions régulières**.
  - d. Définissez le masque ou l'expression dans le champ **Opérateur**.
  - e. Cliquez sur le bouton **OK**.
6. Pour modifier une règle, sélectionnez la règle en question dans la liste et cliquez sur **Modifier**.
7. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles de Contrôle Internet**.

Les nouvelles règles sont appliquées.

## Configuration du Contrôle Internet basé sur les catégories

► *Pour ajouter ou modifier une règle de la Protection du trafic basée sur les catégories :*

1. Ouvrez la fenêtre **Règles de Contrôle Internet** (cf. section "**Ouverture de la fenêtre des règles de protection du trafic**" à la page [334](#)).
2. Ouvrez l'onglet **Catégories**.
3. Cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.

Si la case est cochée, Kaspersky Security for Windows Server définit les catégories des ressources Internet et interdit celles qui appartiennent aux catégories sélectionnées.

Si la case est décochée, Kaspersky Security for Windows Server ne définit pas les catégories.

Cette case est décochée par défaut.

Les paramètres du contrôle de catégorie deviennent disponibles.

4. Cochez ou décochez les cases suivantes :
  - **Autoriser l'accès si la page Internet ne peut pas être classée dans une catégorie.**
  - **Autoriser l'accès aux ressources Internet légitimes qui peuvent servir à nuire au serveur.**
  - **Autoriser l'accès aux publicités légitimes.**
5. Dans la liste des catégories disponibles (cf. section "Liste des catégories" à la page [312](#)) :



- Cochez la case correspondante pour autoriser une catégorie.  
La colonne **Type** passe à l'état **Autorisé**.
- Décochez la case correspondante pour interdire une catégorie.  
La colonne **Type** passe à l'état **Interdit**.

La liste des catégories est prédéfinie et ne peut être modifiée (il est impossible d'ajouter ou de supprimer des catégories).

6. Cliquez sur **Enregistrer**.  
La configuration des règles est enregistrée.

### Utilisation du masque not-a-virus

► Pour utiliser le masque *not-a-virus* dans le cadre de l'analyse d'une catégorie :

1. Dans l'arborescence de la Console de l'application, ouvrez les paramètres de la tâche Utilisation du KSN (cf. section "Configuration de la tâche Utilisation du KSN via la Console de l'application" à la page [302](#)).
2. Cochez la case **Envoyer des données relatives aux URL analysées**.
3. Lancez tâche Utilisation du KSN.
4. Dans la fenêtre de configuration de la Protection du trafic (cf. section "Configuration du mode Intercepteur de pilote" à la page [335](#)), cochez la case **Utiliser KSN pour la protection**.
5. Dans la fenêtre **Règles de Contrôle Internet**, sous l'onglet **Catégories**, cochez la case **Appliquer les règles pour le contrôle des catégories de trafic Internet**.
6. Dans la liste des catégories, sélectionnez les catégories pour lesquelles vous souhaitez appliquer le masque *not-a-virus*.

Les objets des catégories sélectionnées qui correspondent au masque ne seront pas détectés par la tâche Protection du trafic.

L'utilisation du masque not-a-virus est configurée dans les paramètres Zone de confiance.

## Ajout de règles en fonction des adresses Internet

Vous pouvez ajouter une règle en fonction d'une adresse Internet pour autoriser ou interdire une adresse Internet en particulier. Ces règles ont une priorité supérieure à celle de n'importe quelle autre conclusion.

► Pour créer une règle sur la base d'une adresse Internet :

1. Ouvrez la fenêtre **Règles de Contrôle Internet** (cf. section "**Ouverture de la fenêtre des règles de protection du trafic**" à la page [334](#)).
2. Sous l'onglet **Contrôle Internet**, cochez la case **Appliquer les règles basées sur l'URL** pour appliquer les règles.

Si la case est cochée, Kaspersky Security for Windows Server bloque les certificats HTTPS en appliquant les règles d'interdiction personnalisées pour les certificats.

Si la case est décochée, les certificats ne sont pas analysés par l'application.

Cette case est cochée par défaut.

3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
4. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Règle selon l'adresse Internet**.
5. Dans la fenêtre **Règle selon l'adresse Internet** qui s'ouvre :
  - a. Saisissez le nom de la règle.
  - b. Sélectionnez le **Type de règle** : **Interdit** ou **Autorisé**.
  - c. Cochez la case **Appliquer la règle**.
  - d. Indiquez l'URL dans le champ **Adresse Internet**.
  - e. Cliquez sur le bouton **OK**.
6. Pour modifier une règle, sélectionnez la règle en question dans la liste et cliquez sur **Modifier**.
7. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles de Contrôle Internet**.

Les nouvelles règles sont appliquées.

# Protection contre le chiffrement

Cette section contient des informations sur la tâche Protection contre le chiffrement et sur sa configuration.

## Contenu du chapitre

A propos de la tâche Protection contre le chiffrement.....	348
Statistiques de la tâche Protection contre le chiffrement .....	349
Paramètres de la tâche Protection contre le chiffrement par défaut .....	349
Configuration des paramètres de la tâche Protection contre le chiffrement via le Plug-in d'administration .....	350
Configuration des paramètres de la tâche Protection contre le chiffrement via la Console de l'application .....	355

## A propos de la tâche Protection contre le chiffrement

La tâche Protection contre le chiffrement permet de détecter le chiffrement malveillant des ressources de fichier réseau sur un serveur protégé qui provient d'ordinateurs distants sur le réseau de l'entreprise.

Lors de l'exécution de la tâche Protection contre le chiffrement, Kaspersky Security for Windows Server analyse les requêtes des ordinateurs distants adressées aux fichiers qui se trouvent dans les dossiers partagés du serveur protégé. Si l'application considère que les actions d'un ordinateur distant sur des ressources de fichier réseau correspondent à celles d'un chiffrement malveillant, Kaspersky Security for Windows Server ajoute l'identifiant unique local (LUID) de l'ordinateur à la liste d'hôtes bloqués.

La tâche Protection contre le chiffrement peut être exécutée en mode synchrone ou asynchrone. Par défaut, la tâche Protection contre le chiffrement fonctionne en mode asynchrone et le traitement des opérations de fichiers est partagé entre plusieurs flux parallèles. Pour en savoir plus sur les modes synchrones et asynchrones du traitement des opérations de fichier et sur la modification de ce mode, consultez la Banque de solutions de Kaspersky Lab (cf. section "Sources de données pour des consultations indépendantes" à la page [18](#)).

Kaspersky Security for Windows Server ne considère pas qu'il s'agit d'un chiffrement malveillant si l'activité de chiffrement détectée a lieu dans des dossiers exclus de la zone d'action de la tâche Protection contre le chiffrement.

Par défaut, l'application empêche l'accès des ordinateurs bloqués aux ressources de fichier réseau pendant 30 minutes.

**La tâche Protection contre le chiffrement ne bloque pas l'accès aux ressources de fichier réseau tant que l'activité de l'hôte n'est pas considérée comme malveillante. Cela peut durer un certain temps pendant lequel l'application de chiffrement malveillant peut réaliser son activité malveillante.**

Si la tâche Protection contre le chiffrement est lancée en mode Statistiques uniquement, Kaspersky Security for Windows Server consigne uniquement les tentatives de chiffrement malveillant émanant des ordinateurs distants dans le journal d'exécution de la tâche.

## Statistiques de la tâche Protection contre le chiffrement

Quand la tâche Protection contre le chiffrement est en cours d'exécution, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Security for Windows Server depuis son lancement jusqu'à maintenant, autrement dit, les statistiques de l'exécution de la tâche.

► Pour consulter les statistiques de la tâche Protection contre le chiffrement, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Vous pouvez consulter les informations sur les objets que Kaspersky Security for Windows Server a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Tableau 54. Statistiques de la tâche Protection contre le chiffrement

Champ	Description
<b>Détection de tentatives de chiffrement malveillant</b>	Nombre de tentatives d'accès dans lesquelles Kaspersky Security for Windows Server a détecté une activité de chiffrement malveillant.
<b>Erreurs de traitement</b>	Nombre de requêtes d'applications envoyées à la zone de stockage dont le traitement a entraîné une erreur de tâche.
<b>Objets traités</b>	Nombre de tentatives d'accès traitées par Kaspersky Security for Windows Server.

## Paramètres de la tâche Protection contre le chiffrement par défaut

La tâche Protection contre le chiffrement

utilise les paramètres par défaut décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 55. Paramètres de la tâche Protection contre le chiffrement par défaut

Paramètre	Valeur par défaut	Description
<b>Mode de travail</b>	Actif	La tâche Protection contre le chiffrement peut être lancée en mode <b>Actif</b> ou <b>Statistiques uniquement</b> .
<b>Zone de protection</b>	Kaspersky Security for Windows Server applique la tâche Protection contre le chiffrement à tous les dossiers partagés du serveur par défaut.	Vous pouvez modifier la zone de protection en indiquant les dossiers partagés auxquels doit s'appliquer la tâche.

Paramètre	Valeur par défaut	Description
<b>Exclusions</b>	La liste d'exclusion est appliquée et inclut des éléments ajoutés par les experts de Kaspersky Lab.	Spécifiez les zones que vous souhaitez inclure dans la zone de protection de la tâche.
<b>Analyse heuristique</b>	L'analyse heuristique est activée et Kaspersky Security for Windows Server applique le niveau d'analyse <b>Moyenne</b> .	Vous pouvez activer ou désactiver l'analyse heuristique et régler le niveau de détail de l'analyse.
<b>Paramètres de planification</b>	Par défaut, le premier lancement n'est pas défini. La tâche Protection contre le chiffrement n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server.	Vous pouvez lancer la tâche manuellement ou planifier son exécution.



## Configuration des paramètres de la tâche Protection contre le chiffrement via le Plug-in d'administration

► *Pour configurer les paramètres de la tâche Protection contre le chiffrement, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre le chiffrement** subsection.
- La fenêtre **Protection contre le chiffrement** s'ouvre.
5. Configurez les paramètres suivants dans la fenêtre qui s'ouvre :
    - Utilisation du mode Tâche et de l'analyseur heuristique (cf. section "Paramètres généraux de la tâche" à la page [351](#)) sous l'onglet **Général**.
    - Zone de protection (cf. section "Constitution de la zone de protection" à la page [352](#)) sous l'onglet **Zone**

## de protection.

- Exclusions (cf. section "Ajout d'exclusions" à la page [353](#)) sous l'onglet **Exclusions**.
- Paramètres de lancement de la tâche planifiée (cf. section "Programmation des tâches" à la page [138](#)) sous l'onglet **Administration des tâches**.

6. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

## Dans cette section

Paramètres des tâches de groupe .....	<a href="#">351</a>
Constitution de la zone de protection .....	<a href="#">352</a>
Ajout d'exclusions .....	<a href="#">353</a>

## Paramètres des tâches de groupe

► *Pour configurer les paramètres d'une tâche locale :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre le chiffrement** subsection.

La fenêtre **Protection contre le chiffrement** s'ouvre.

5. Dans la section **Mode de travail** de l'onglet **Général**, sélectionnez le mode **Actif**.

En cas de détection d'un chiffrement malveillant, Kaspersky Security for Windows Server

interdit l'accès aux dossiers partagés des ordinateurs compromis.

6. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

7. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

Il existe trois niveaux de détail pour l'analyse

- **Superficielle.** L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
- **Moyenne.** L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.  
Il s'agit du niveau par défaut.
- **Minutieuse.** L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

8. Cliquez sur le bouton **OK** pour appliquer la nouvelle configuration.

## Constitution de la zone de protection

La tâche de protection contre le chiffrement accepte les types de zone de protection suivants :

- **Prédéfinie.** Vous pouvez utiliser la zone de protection définie par défaut et qui reprend tous les dossiers partagés du serveur. Cette valeur est appliquée si le paramètre **Tous les dossiers réseau partagés du serveur** est sélectionné.
- **Utilisateur.** Vous pouvez configurer vous-même la zone de protection en sélectionnant les dossiers à inclure dans la zone de protection contre le chiffrement malveillant. Cette valeur est appliquée quand le paramètre **Uniquement les dossiers partagés indiqués** est sélectionné.

**Vous pouvez utiliser le chemin d'accès local pour configurer la zone de protection de la tâche Protection contre le chiffrement.**

► *Pour configurer une zone de protection pour la tâche Protection contre le chiffrement, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de

Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre le chiffrement** subsection.

La fenêtre **Protection contre le chiffrement** s'ouvre.

5. Dans la section **Zone de protection**, sélectionnez les dossiers que Kaspersky Security for Windows Server va analyser dans le cadre de l'exécution de la tâche Protection contre le chiffrement :

- **Tous les dossiers réseau partagés du serveur.**

Si vous avez choisi cette option, Kaspersky Security for Windows Server analyse tous les dossiers partagés du serveur lors de l'exécution de la tâche Protection contre le chiffrement.

Cette option est sélectionnée par défaut.

- **Uniquement les dossiers partagés indiqués.**

Si vous avez choisi cette option, Kaspersky Security for Windows Server analyse uniquement les dossiers partagés que vous avez désignés manuellement lors de l'exécution de la tâche Protection contre le chiffrement.

6. Pour spécifier les dossiers partagés du serveur que vous souhaitez inclure dans la zone de protection contre le chiffrement malveillant :

- a. Sélectionnez **Uniquement les dossiers partagés indiqués**, puis cliquez sur le bouton **Ajouter**.

La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.

- b. Cliquez sur le bouton **Parcourir** pour sélectionner un dossier ou entrez manuellement le dossier.
- c. Cliquez sur le bouton **OK**.

7. Dans la fenêtre **Protection contre le chiffrement**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Ajout d'exclusions

- Pour ajouter des exclusions de la zone de protection contre le chiffrement malveillant, procédez



comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre le chiffrement** subsection.

La fenêtre **Protection contre le chiffrement** s'ouvre.

5. Sous l'onglet **Exclusions**, cochez la case **Appliquer la liste d'exclusions**.

Si la case est cochée, Kaspersky Security for Windows Server ne détecte pas le chiffrement malveillant dans les zones définies lors de l'exécution de la tâche Protection contre le chiffrement.

Si la case est décochée, Kaspersky Security for Windows Server détecte les activités de chiffrement malveillant pour tous les dossiers partagés.

Par défaut, la case est cochée et la liste d'exclusion inclut les éléments suivants ajoutés par les experts de Kaspersky Lab :

- \*.stt ;
- \*.sig ;
- \*.exe ;
- \*.sldprt.

6. Cliquez sur **Ajouter**.

La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.

7. Cliquez sur le bouton **Parcourir** pour sélectionner un dossier ou entrez manuellement le dossier.
8. Cliquez sur le bouton **OK**.

La zone exclue est ajoutée à la liste.

## Configuration des paramètres de la tâche Protection contre le chiffrement via la Console de l'application

► Pour configurer les paramètres de la tâche Protection contre le chiffrement, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.
3. Dans le panneau de détails du nœud **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**. La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez les paramètres suivants dans la fenêtre qui s'ouvre :
  - Utilisation du mode de travail et de l'analyse heuristique (cf. section "Paramètres généraux de la tâche" à la page [357](#)) sous l'onglet **Général**.
  - Zone de protection (cf. section "Constitution de la zone de protection" à la page [355](#)) sous l'onglet **Zone de protection**.
  - Exclusions (cf. section "Ajout d'exclusions" à la page [357](#)) sous l'onglet **Exclusions**.
  - Paramètres de lancement de la tâche planifiée (cf. section "Programmation des tâches" à la page [138](#)) sous les onglets **Planification** et **Avancé**.
5. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

### Dans cette section

Constitution de la zone de protection .....	<a href="#">355</a>
Paramètres des tâches de groupe .....	<a href="#">357</a>
Ajout d'exclusions .....	<a href="#">357</a>

## Constitution de la zone de protection

La tâche de protection contre le chiffrement accepte les types de zone de protection suivants :

- **Prédéfinie**. Vous pouvez utiliser la zone de protection définie par défaut et qui reprend tous les dossiers réseau partagés du serveur. Cette valeur est appliquée si le paramètre **Tous les dossiers réseau partagés du serveur** est sélectionné.
- **Utilisateur**. Vous pouvez configurer vous-même la zone de protection en sélectionnant les dossiers à inclure dans la zone de protection contre le chiffrement malveillant. Cette valeur est appliquée quand le paramètre **Uniquement les dossiers partagés indiqués** est sélectionné.

Vous pouvez utiliser le chemin d'accès local pour configurer la zone de protection de la tâche Protection contre le chiffrement.

Que ce soit lors de l'utilisation d'une zone de protection prédéfinie ou définie par l'utilisateur, il est possible d'exclure des dossiers sélectionnés de la zone de protection, par exemple si les données de ces dossiers sont chiffrées à l'aide d'applications installées sur des périphériques distants.

► *Pour configurer une zone de protection pour la tâche Protection contre le chiffrement, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.
3. Dans le panneau de détails du nœud **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la section **Zone de protection**, sélectionnez les dossiers que Kaspersky Security for Windows Server va analyser dans le cadre de l'exécution de la tâche Protection contre le chiffrement :

- **Tous les dossiers réseau partagés du serveur.**

Si vous avez choisi cette option, Kaspersky Security for Windows Server analyse tous les dossiers partagés du serveur lors de l'exécution de la tâche Protection contre le chiffrement.

Cette option est sélectionnée par défaut.

- **Uniquement les dossiers partagés indiqués.**

Si vous avez choisi cette option, Kaspersky Security for Windows Server analyse uniquement les dossiers partagés que vous avez désignés manuellement lors de l'exécution de la tâche Protection contre le chiffrement.

5. Pour spécifier les dossiers partagés du serveur que vous souhaitez inclure dans la zone de protection contre le chiffrement malveillant, utilisez une des méthodes suivantes :
  - Manuellement :
    - a. Entrez le nom du dossier partagé sur un serveur protégé.
    - b. Cliquez sur **Ajouter**.  
Le dossier est ajouté à la liste.
  - A l'aide de la recherche :
    - a. Cliquez sur le bouton **Parcourir**.  
La fenêtre standard de Microsoft Windows s'ouvre.
    - b. Sélectionnez le dossier que vous souhaitez ajouter à la zone de protection de la tâche.
    - c. Cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Paramètres des tâches de groupe

► *Pour configurer les paramètres d'une tâche locale :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.
3. Dans le panneau de détails du nœud **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

4. Dans la section **Mode de travail** de l'onglet **Général**, sélectionnez le mode **Actif**.

En cas de détection d'un chiffrement malveillant, Kaspersky Security for Windows Server interdit l'accès aux dossiers partagés des ordinateurs compromis.

5. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

6. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse.

Il existe trois niveaux de détail pour l'analyse

- **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement.
- **Moyenne**. L'analyseur heuristique exécute le nombre d'instructions dans le fichier exécutable recommandé par les experts de Kaspersky Lab.  
Il s'agit du niveau par défaut.
- **Minutieuse**. L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

7. Cliquez sur le bouton **OK** pour appliquer la nouvelle configuration.

## Ajout d'exclusions

► *Pour configurer une zone de protection pour la tâche Protection contre le chiffrement, procédez*

comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel du serveur**.
2. Sélectionnez le nœud enfant **Protection contre le chiffrement**.
3. Dans le panneau de détails du nœud **Protection contre le chiffrement**, cliquez sur le lien **Propriétés**. La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Exclusions**, cochez la case **Appliquer la liste d'exclusions**.

Si la case est cochée, Kaspersky Security for Windows Server ne détecte pas le chiffrement malveillant dans les zones définies lors de l'exécution de la tâche Protection contre le chiffrement.

Si la case est décochée, Kaspersky Security for Windows Server détecte les activités de chiffrement malveillant pour tous les dossiers partagés.

Par défaut, la case est cochée et la liste d'exclusion inclut les éléments suivants ajoutés par les experts de Kaspersky Lab :

- \*.stt ;
- \*.sig ;
- \*.exe ;
- \*.sldprt.

5. Indiquez un nom de dossier ou un masque.
6. Cliquez sur **Ajouter**.
7. Le cas échéant, répétez les étapes 5 et 6 pour ajouter d'autres exclusions.
8. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les exclusions de la zone de protection sont ajoutées et appliquées.

# Contrôle du lancement des applications

Cette section contient des informations sur la tâche de Contrôle du lancement des applications et les instructions sur la configuration de cette tâche.

## Contenu du chapitre

A propos de la tâche Contrôle du lancement des applications .....	<a href="#">359</a>
A propos des règles du Contrôle du lancement des applications .....	<a href="#">360</a>
A propos du contrôle de la distribution des logiciels.....	<a href="#">362</a>
A propos l'utilisation du KSN dans la tâche Contrôle du lancement des applications .....	<a href="#">365</a>
Création des règles du Contrôle du lancement des applications .....	<a href="#">366</a>
Paramètres de la tâche Contrôle du lancement des applications par défaut .....	<a href="#">368</a>
Administration du Contrôle du lancement des applications via le plug-in d'administration .....	<a href="#">371</a>
Administration du Contrôle du lancement des applications via la Console de l'application .....	<a href="#">396</a>

## A propos de la tâche Contrôle du lancement des applications

Dans le cadre de la tâche Contrôle du lancement des applications, Kaspersky Security for Windows Server surveille les tentatives de lancement d'applications par l'utilisateur et autorise ou refuse ces lancements. La tâche Contrôle du lancement des applications repose sur le principe Interdire par défaut, ce qui signifie que toute application qui n'est pas autorisée dans les paramètres de la tâche sera bloquée automatiquement.

Vous pouvez autoriser le lancement des applications d'une des manières suivantes :

- définir des règles d'autorisation pour les applications de confiance ;
- Vérifier la réputation des applications de confiance dans KSN au moment de leur lancement.

La tâche accorde la plus haute priorité à l'interdiction du lancement des applications : si le lancement d'une application est interdit par l'une des règles de blocage, le lancement de l'application est interdit quelle que soit la conclusion de confiance de KSN. Par exemple, si les services KSN considèrent que l'application est douteuse, mais qu'elle est couverte par une règle d'autorisation, le démarrage de cette application sera interdit.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution de la tâche (cf. section "A propos des journaux d'exécution des tâches" à la page [216](#)).

Le Contrôle du lancement des applications s'opère selon un des deux modes suivants :

- **Actif.** Kaspersky Security for Windows Server contrôle, à l'aide de règles définies, le lancement des applications qui font partie de la zone d'application des règles du Contrôle du lancement des applications.

La zone d'application des règles du Contrôle du lancement des applications peut être définie dans les paramètres de cette tâche. Si une application entre dans la zone d'application des règles du Contrôle du lancement des applications, et que les paramètres de la tâche ne respectent aucune des règles définie, le lancement de cette application sera interdit.

Le lancement des applications n'entrant pas dans la zone d'application d'aucune règle définie dans les paramètres de la tâche Contrôle du lancement des applications est autorisé, indépendamment des paramètres de la tâche Contrôle du lancement des applications.

Il est impossible de lancer la tâche **Contrôle du lancement des applications** en mode Actif, si aucune règle n'a été créée ou s'il existe plus de 65 535 règles pour un serveur.

- **Statistiques uniquement.** Kaspersky Security for Windows Server ne prend pas en charge les règles du Contrôle du lancement des applications pour autoriser ou interdire le lancement des applications. Il se content d'enregistrer les informations relatives aux lancements des applications, aux règles respectées par l'exécution des applications et aux actions qui auraient été exécutées si la tâche avait été lancée en mode **Actif**. Le lancement de toutes les applications est autorisé. Il s'agit du mode par défaut.

Vous pouvez utiliser ce mode pour créer les règles du Contrôle du lancement des applications (cf. section "Création de règles d'autorisation au départ des événements de la tâche Contrôle du lancement des applications" à la page [408](#)) sur la base des informations consignées dans le journal d'exécution de la tâche.

Vous pouvez configurer le fonctionnement de la tâche Contrôle du lancement des applications conformément à un des scénarios suivants :

- Configuration de règle avancée (cf. section "A propos des règles du Contrôle du lancement des applications" à la page [360](#)) et leur utilisation dans le cadre du Contrôle du lancement des applications.
- Configuration des règles de base et utilisation du KSN (cf. section "Configuration de l'utilisation du KSN" à la page [401](#)) pour le Contrôle du lancement des applications.

Si des fichiers du système d'exploitation sont couverts par la tâche de Contrôle du lancement des applications, il est conseillé, lors de la création des règles du Contrôle du lancement des applications, de confirmer que ces applications sont autorisées par les nouvelles règles. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Kaspersky Security for Windows Server intercepte également les processus lancés sous le Sous-système Windows pour Linux (sauf les scripts exécutés à partir du shell UNIX™ ou d'interpréteurs de ligne de commande). Pour ces processus, la tâche Contrôle du lancement des applications applique l'action définie par la configuration en cours. La tâche Génération des règles du Contrôle du lancement des applications détecte les lancements de l'application et génère les règles correspondantes pour les application exécutées sous le Sous-système Windows pour Linux.

## A propos des règles du contrôle du lancement des applications

### Principe de fonctionnement des règles du Contrôle du lancement des applications

Le fonctionnement des règles du Contrôle du lancement des applications est basé sur les composantes suivantes :

- Type de règle.

Les règles du Contrôle du lancement des applications peuvent autoriser ou interdire le lancement de l'application. Pour cette raison, il peut s'agir de règles *d'autorisation* ou de règles *d'interdiction*. Pour créer une liste de règles d'autorisation du Contrôle du lancement des applications, vous pouvez utiliser la tâche de génération des règles d'autorisation ou la tâche Contrôle du lancement des applications en mode **Statistiques uniquement**. Il est également possible d'ajouter des règle d'autorisation manuellement.

- Utilisateur et/ou groupe d'utilisateurs.

Les règles du Contrôle du lancement des applications contrôlent les lancements des applications définies par l'utilisateur et / ou le groupe d'utilisateurs.

- Zone d'application des règles.

Les règles du Contrôle du lancement des applications peuvent s'appliquer aux *fichiers exécutables des applications*, aux *scripts* et aux *paquets MSI*.

- Critères de déclenchement de la règle.

Les règles du Contrôle du lancement des applications contrôlent le lancement des fichiers répondant à un critère défini dans les paramètres de la règle : signés par le *certificat numérique* indiqué, correspondant au *hash SHA256* indiqué ou sont situés sur le *chemin* indiqué.

Si le critère de déclenchement de la règle est le paramètre **Certificat numérique**, la règle créée contrôle le lancement de n'importe quelle application de confiance dans le système d'exploitation. Vous pouvez créer des conditions plus strictes pour ce critère en cochant les cases suivantes :

- **Utiliser l'objet**

La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que critère de déclenchement de la règle.

Si la case est cochée, l'objet du certificat numérique indiqué sera utilisé en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications uniquement pour l'éditeur repris dans l'en-tête.

Si la case est décochée, l'application n'utilise pas les en-têtes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, la règle créée contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quel en-tête.

L'en-tête du certificat numérique utilisé pour signer le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**

La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de déclenchement de la règle.

Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications signées par le certificat numérique doté de l'empreinte indiquée.

Si la case est décochée, l'application n'utilise pas l'empreinte de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, l'application contrôlera le lancement des applications signées à l'aide du certificat numérique doté n'importe quelle empreinte.



L'empreinte du certificat numérique utilisé pour signer le fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

L'empreinte limite de manière plus stricte le déclenchement des règles de lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée, à la différence de l'en-tête du certificat numérique.

Vous pouvez définir des exclusions pour une règle du Contrôle du lancement des applications. Les exclusions d'une règle du Contrôle du lancement des applications sont basées sur les mêmes critères que ceux déclenchant les règles : certificat numérique, hash SHA256 ou chemin d'accès au fichier. Des exclusions des règles du Contrôle du lancement des applications peuvent se justifier pour certaines règles d'autorisation : par exemple, si vous souhaitez permettre aux utilisateurs de lancer les applications depuis le chemin C:\Windows, mais que vous souhaitez interdire l'exécution du fichier Regedit.exe.

Si des fichiers du système d'exploitation sont couverts par la tâche de Contrôle du lancement des applications, il est conseillé, lors de la création des règles du Contrôle du lancement des applications, de confirmer que ces applications sont autorisées par les nouvelles règles. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

### Administration des règles du Contrôle du lancement des applications

Vous pouvez réaliser les opérations suivantes au niveau des règles du Contrôle du lancement des applications :

- Ajouter les règles manuellement.
- Créer et ajouter des règles automatiquement.
- Supprimer les règles.
- Exporter des règles dans un fichier de configuration.
- Vérifier si les fichiers sélectionnés contiennent des règles d'autorisation de leur lancement.
- Filtrer la liste des règles selon le critère spécifié.

## A propos du contrôle de la distribution des logiciels

La création de règles du Contrôle du lancement des applications peut s'avérer complexe s'il faut contrôler également la distribution de logiciels sur un serveur protégé, par exemple sur les serveurs où le logiciel installé est automatiquement mis à jour à intervalles réguliers. Dans ce cas, la liste de règles d'autorisation doit être mise à jour après chaque mise à jour de logiciel afin que les fichiers juste créés soient pris en compte dans les paramètres de la tâche Contrôle du lancement des applications. Pour simplifier le contrôle du lancement dans les scénarios de distribution des logiciels, vous pouvez utiliser le sous-système Contrôle de la distribution des logiciels.

Un *paquet de distribution des logiciels* (ci-après appelé "paquet") représente une application logicielle à installer sur un serveur. Chaque paquet contient au moins une application et peut également contenir des fichiers séparés, des mises à jour, voire une commande séparée en plus des applications, notamment lorsque vous installez une

application ou une mise à jour logicielle.

Le sous-système Contrôle de la distribution des logiciels est mis en œuvre en tant que liste supplémentaire d'exclusions. Quand vous ajoutez un paquet de distribution de logiciels à cette liste, l'application autorise la décompression de ces paquets de confiance ainsi que le lancement automatique de l'installation ou la modification par un paquet de confiance. Les fichiers extraits peuvent hériter de l'attribut de confiance du paquet de distribution principal. Un *paquet de distribution principal* est un paquet qui a été ajouté à la liste d'exclusions du Contrôle de la distribution des logiciels par l'utilisateur et qui est devenu un paquet de confiance.

Kaspersky Security for Windows Server contrôle uniquement les cycles de distribution de logiciels complets. L'application ne peut pas traiter correctement le lancement des fichiers qui sont modifiés par un paquet de confiance si, lors du premier lancement du paquet, le Contrôle de la distribution des logiciels est désactivé ou si le composant Contrôle du lancement des applications n'est pas installé.

Le Contrôle de la distribution de logiciels n'est pas disponible si la case **Utiliser les règles pour les fichiers exécutables** est décochée dans les paramètres de la tâche Contrôle du lancement des applications.

### Cache de la distribution des logiciels

Kaspersky Security for Windows Server établit le rapport entre les paquets de confiance et les fichiers créés lors de la distribution des logiciels à l'aide d'un cache de la distribution des logiciels généré automatiquement ("cache de distribution"). Au premier lancement d'un paquet, Kaspersky Security for Windows Server détecte tous les fichiers créés par ce paquet lors de du processus de distribution de logiciels et stocke les sommes de contrôles et les chemins d'accès des fichiers dans le cache de distribution. Ensuite, le lancement de tous les fichiers repris dans le cache de distribution est autorisé par défaut.

Vous ne pouvez pas réviser, effacer ou modifier manuellement le cache de distribution via l'interface utilisateur. Le cache est rempli et contrôlé par Kaspersky Security for Windows Server.

Vous pouvez exporter le cache de distribution dans un fichier de configuration (au format XML) et aussi effacer le cache à l'aide des options de ligne de commande.

- *Pour exporter le cache de distribution dans un fichier de configuration, exécutez la commande suivante :*

```
kavshell appcontrol /config /savetofile:<chemin complet> /sdc
```

- *Pour effacer le cache de distribution, exécutez la commande suivante :*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Security for Windows Server met à jour le cache de distribution toutes les 24 heures. En cas de modification de la somme de contrôle d'un fichier qui était autorisé, l'application supprime l'enregistrement de ce fichier dans le cache de distribution. Si la tâche Contrôle du lancement des applications est lancée en mode actif, les tentatives de lancement ultérieures de ce fichier sont bloquées. Si le chemin complet d'accès au fichier précédemment autorisé est modifié, les tentatives ultérieures de lancer ce fichier ne seront pas bloquées car la somme de contrôle est stockée dans le cache de distribution.

## Traitement des fichiers extraits

Tous les fichiers extraits d'un paquet de confiance hérite de l'attribut de confiance au premier lancement du paquet. Si vous décochez la case après le premier lancement, tous les fichiers extraits du paquet conservent l'attribut hérité. Pour réinitialiser l'attribut hérité sur tous les fichiers extraits, vous devez effacer le cache de distribution et décocher la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution** avant de redémarrer le paquet de distribution de confiance.

Les fichiers extraits et les paquets, créés par un paquet de distribution principal de confiance, acquièrent l'attribut de confiance quand leurs sommes de contrôle sont ajoutées au cache de distribution lorsque le paquet de distribution de logiciels de la liste d'exclusions est ouvert pour la première fois. Par conséquent, le paquet de distribution proprement dit et tous les fichiers inclus sont également de confiance. Par défaut, le nombre de niveaux d'héritage d'attribut de confiance est illimité.

Les fichiers extraits conservent l'attribut de confiance après le redémarrage du système d'exploitation.

Pour configurer le traitement des fichiers dans les paramètres du Contrôle de la distribution des logiciels (cf. section "Configuration du Contrôle de la distribution des logiciels" à la page [376](#)), vous devez cocher ou décocher la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**.

Par exemple, supposons que vous ajoutez un paquet test.msi contenant plusieurs autres paquets et applications à la liste d'exclusions et cochez la case. Dans ce cas, tous les paquets et applications contenus dans le paquet test.msi peuvent être exécutés ou extraits s'ils contiennent d'autres fichiers. Ce scénario est valable pour les fichiers extraits sur tous les niveaux imbriqués.

Si vous ajoutez un paquet test.msi à la liste d'exclusions et décochez la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**, l'application affecte l'attribut de confiance uniquement aux paquets et aux fichiers exécutables extraits directement d'un paquet de confiance principal (imbriqué au premier niveau). Les sommes de contrôle de ces fichiers sont stockées dans le cache de distribution. Tous les fichiers imbriqués au second niveau et plus sont bloqués par le principe Interdire par défaut.

### Utilisation de la liste des règles de contrôle du lancement des applications

La liste des paquets de confiance du sous-système de contrôle de la distribution des logiciels est une liste d'exclusions, ce qui amplifie, mais ne remplace pas la liste générale de règles de contrôle du lancement des applications.

Les règles d'interdiction de contrôle du lancement des applications a la priorité la plus élevée : la décompression des paquets de confiance et le démarrage de fichiers nouveaux ou modifiés sont bloqués si ces paquets et fichiers sont affectés par les règles d'interdiction du contrôle du lancement des applications.

Les exclusions de contrôle de la distribution des logiciels sont appliquées à la fois pour les paquets de confiance et les fichiers créés ou modifiés par ces paquets si aucune règle d'interdiction dans la liste de contrôle du lancement des applications n'est appliquée pour ces paquets et fichiers.

### Utilisation des conclusions KSN

Les conclusions de KSN sur le caractère douteux d'un fichier ont priorité sur les exclusions du Contrôle de la distribution des logiciels : la décompression des paquets de confiance et le lancement des fichiers créés ou modifiés par ces paquets sont interdits si KSN signale que ces fichiers sont douteux.

## A propos l'utilisation du KSN dans la tâche Contrôle du lancement des applications

Vous devez accepter la Déclaration de KSN afin de lancer la tâche Utilisation du KSN.

Si les données de KSN relatives à la réputation d'une application sont utilisées par la tâche du Contrôle du lancement des applications, la réputation de l'application selon KSN est considérée comme un critère d'autorisation ou d'interdiction du lancement de cette application. Si KSN signale à Kaspersky Security for Windows Server qu'une application est douteuse lorsque l'utilisateur tente de la lancer, le lancement est refusé. Si KSN signale à Kaspersky Security for Windows Server qu'une application est de confiance lorsque l'utilisateur tente de la lancer, le lancement est autorisé. Vous pouvez appliquer KSN avec les règles du Contrôle du lancement des applications ou à titre de critère indépendant pour interdire le lancement des applications.

### Application des conclusions du KSN en tant que critère indépendant de l'interdiction du lancement des applications

Ce scénario permet de contrôler sans danger le lancement des applications sur un serveur protégé sans configuration avancée de la liste des règles.

Vous pouvez appliquer les conclusions du KSN à Kaspersky Security for Windows Server avec la seule règle définie. L'application autorisera uniquement le lancement d'applications considérées comme des applications de confiance dans KSN ou qui sont autorisées par une règle définie.

Si vous adoptez ce scénario, il est conseillé de définir une règle d'autorisation du lancement des applications selon un certificat numérique.

Toutes les autres applications seront bloquées conformément à la stratégie Interdire par défaut. L'application du KSN en l'absence de règles permet de protéger l'ordinateur contre les applications qui constituent une menace d'après KSN.

### Application des conclusions du KSN avec les règles du Contrôle du lancement des applications

Lors de l'utilisation des conclusions du KSN avec les règles du Contrôle du lancement des applications, les conditions suivantes s'appliquent :

- Kaspersky Security for Windows Server interdit toujours le lancement d'une application si elle est couverte par au moins une règle d'interdiction. Si l'application est considérée comme une application de confiance par KSN, la conclusion correspondante possède une priorité inférieure et n'est pas prise en compte ; le lancement l'application sera toujours interdit. Cela permet de développer la liste des applications indésirables.
- Kaspersky Security for Windows Server interdit toujours le lancement d'une application si le lancement est interdit pour les applications considérées comme douteuses dans KSN et qu'il s'avère que cette application est considérée comme douteuse dans KSN. Si une règle d'autorisation a été définie pour l'application, elle possède une priorité inférieure et n'est pas prise en compte ; l'application sera de toute manière interdite. Cela permet de protéger l'ordinateur contre les applications qui constituent une menace d'après les données du KSN et qui n'ont pas été prises en considération lors de la configuration initiale des règles.

## Création des règles du Contrôle du lancement des applications

Vous pouvez créer des listes de règles du Contrôle du lancement des applications à l'aide de tâches et de stratégies de Kaspersky Security Center simultanément pour tous les serveurs et groupes de serveurs du réseau de l'organisation. Ce scénario est recommandé si le réseau de l'entreprise ne contient pas une machine de référence et si vous ne parvenez pas à créer une liste de règles d'autorisation sur la base des applications installées sur la machine de référence. Il est possible également de lancer localement la tâche Génération des règles du Contrôle du lancement des applications via la Console de l'application pour créer une liste de règle en fonction des applications exécutées sur un seul serveur.

Le composant Contrôle du lancement des applications est installé avec deux règles d'autorisation prédéfinies :

- Règle d'autorisation pour les scripts et les fichiers MSI dotés d'un certificat reconnu par le système d'exploitation.
- Règle d'autorisation pour les fichiers exécutables dotés d'un certificat reconnu par le système d'exploitation.

Vous pouvez créer des listes de règles du Contrôle du lancement des applications dans Kaspersky Security Center d'une des manières suivantes :

- Avec l'aide d'une tâche de groupe Génération des règles du Contrôle du lancement des applications.

Dans ce scénario, une tâche de groupe crée pour chaque serveur du réseau sa propre liste de règles du Contrôle du lancement des applications et les enregistre dans un fichier XML dans le dossier partagé indiqué. Le fichier XML créé par la tâche Génération des règles du Contrôle du lancement des applications contient les règles d'autorisation définies dans les paramètres de la tâche avant le lancement de la tâche. Aucune règle ne sera créée pour les applications dont le lancement n'est pas autorisé par les paramètres définis de la tâche. Le lancement de ces applications est interdit par défaut. Par la suite, vous pouvez importer manuellement les listes de règles créées dans la tâche Contrôle du lancement des applications pour la stratégie Kaspersky Security Center. Vous pouvez ajouter automatiquement les règles créées à la liste des règles de Contrôle du lancement des applications à la fin de la tâche de groupe Génération des règles du Contrôle du lancement des applications.

Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles de la tâche Contrôle du lancement des applications.

Il est conseillé d'utiliser ce scénario quand il faut créer rapidement des listes de règles du Contrôle du lancement des applications. Nous conseillons de configurer le lancement de la tâche Génération des règles du Contrôle du lancement des applications selon une planification uniquement si la zone d'application des règles d'autorisation contient des dossiers et des fichiers réputés sûrs.

Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier partagé n'est pas prévue par la stratégie de l'organisation, nous vous conseillons de lancer la tâche Génération des règles du Contrôle du lancement des applications sur un serveur appartenant au groupe de serveurs d'essai ou sur une machine modèle.

- Sur la base du rapport relatif aux événements de la tâche généré dans Kaspersky Security Center pour le fonctionnement du Contrôle du lancement des applications en mode **Statistiques uniquement**.

Dans le cadre de ce scénario, Kaspersky Security for Windows Server n'interdit pas le lancement des applications. Au contraire, alors que le Contrôle du lancement des applications fonctionne en mode **Statistiques uniquement**, il signale toutes les interdictions et autorisation de lancement d'application sur l'ensemble des serveurs du réseau dans la section **Événements** de Kaspersky Security Center. Kaspersky

Security Center crée une liste unique d'événements caractérisés par l'interdiction du lancement de l'application sur la base du journal d'exécution de la tâche.

Il faut configurer la période d'exécution de la tâche de telle sorte que tous les scénarios envisageables qui impliquent tous les serveurs à protéger et les groupes de serveurs ainsi qu'au moins le redémarrage d'un serveur puisse être réalisé au cours de l'intervalle indiqué. Après l'ajout de règles à la tâche du Contrôle du lancement des applications, vous pouvez importer les données relatives aux lancements d'application depuis le fichier de rapport sur les événements de Kaspersky Security Center enregistré au format TXT et créer, sur la base de ces données, des règles d'autorisation pour le contrôle du lancement de ces applications.

Il est recommandé d'utiliser ce scénario quand le réseau de l'organisation compte un nombre élevé d'ordinateurs de différents types (cf. section "Utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center" à la page [395](#)) (avec différentes applications installées).

- Sur la base des événements d'interdiction de lancement des applications reçus via Kaspersky Security Center, sans création et importation du fichier de configuration.

Pour pouvoir exploiter cette possibilité, la tâche Contrôle du lancement des applications sur l'ordinateur local doit être placée sous une stratégie active de Kaspersky Security Center. Dans ce cas, tous les événements sur l'ordinateur local sont transmis au Serveur d'administration.

Nous conseillons d'actualiser les listes de règles après toute modification de la composition des applications installées sur les serveurs du réseau (par exemple, en cas d'installation d'une mise à jour ou de réinstallation du système d'exploitation). Il est conseillé de créer une liste mise à jour de règles en exécutant la tâche Génération des règles du Contrôle du lancement des applications ou la tâche Contrôle du lancement des applications en mode **Statistiques uniquement** sur les serveurs du groupe d'administration test. Le groupe d'administration d'essai réunit les serveurs indispensables à la vérification du lancement de nouvelles applications avant leur installation sur les serveurs du réseau.

Les fichiers XML qui contiennent la liste des règles d'autorisation, sont créés sur la base de l'analyse des tâches lancées sur le serveur à protéger. Pour comptabiliser toutes les applications utilisées sur le réseau lors de la création des listes de règles, il est conseillé de lancer la tâche Génération des règles du Contrôle du lancement des applications en mode **Statistiques uniquement** sur une machine de référence.

Avant de créer des règles d'autorisation sur la base des applications lancées sur une machine de référence, assurez-vous que celle-ci est sûre et qu'elle n'est infectée par aucune application malveillante.

Avant d'ajouter des règles d'autorisation, sélectionnez un des modes d'application de règle disponible. La liste des règles de la stratégie de Kaspersky Security Center affiche uniquement les règles définies dans cette stratégie, quel que soit le mode d'application des règles. La liste des règles locale affiche toutes les règles appliquées, quelles soient locales ou ajoutées via une stratégie.

## Paramètres de la tâche Contrôle du lancement des applications par défaut

La tâche Contrôle du lancement des applications possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 56. Paramètres de la tâche Contrôle du lancement des applications par défaut

Paramètre	Valeur par défaut	Description
<b>Mode de tâche</b>	<b>Statistiques uniquement.</b> La tâche enregistre les lancements interdits et autorisés sur la base des règles définies. Le lancement de l'application n'est pas interdit.	Vous pouvez sélectionner le mode <b>Actif</b> après la création de la liste définitive des règles.
<b>Répéter les actions adoptées au premier lancement du fichier à tous ses lancements ultérieurs</b>	Appliquée.	Vous pouvez répéter les actions adoptées au premier lancement du fichier à tous ses lancements ultérieurs.
<b>Interdire le lancement de l'interpréteur de ligne de commande sans commande à exécuter</b>	Pas appliqué.	Vous pouvez interdire le lancement des interpréteurs de ligne commande sans commande à exécuter.
<b>Gestion des règles</b>	<b>Remplacer les règles locales par les règles de la stratégie</b>	Vous pouvez choisir le mode d'application commune des règles spécifiées dans la stratégie et les règles sur l'ordinateur local.
<b>Zone d'application des règles</b>	La tâche contrôle l'exécution des fichiers exécutables, des scripts et des paquets MSI.	Vous pouvez indiquer les types de fichier dont le lancement sera contrôlé par les règles.
<b>Utilisation du KSN</b>	Les données de KSN relatives à la réputation des applications ne sont pas utilisées.	Vous pouvez utiliser les données sur la réputation des applications de KSN dans le fonctionnement de la tâche Contrôle du lancement des applications.



Paramètre	Valeur par défaut	Description
<b>Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste</b>	Pas appliqué.	Vous pouvez autoriser la diffusion de l'application à l'aide des paquets d'installation et des applications indiqués dans les paramètres. Par défaut, seule l'autorisation des applications à l'aide du service Windows Installer est autorisée.
<b>Toujours autoriser la diffusion de logiciel via Windows Installer</b>	Appliqué (peut être modifié uniquement lorsque le paramètre <b>Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste</b> est activé).	Vous pouvez autoriser l'installation ou la mise à jour de n'importe quel logiciel si les opérations sont exécutées via Windows Installer.
<b>Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)</b>	Non appliqué (peut être modifié uniquement lorsque le paramètre <b>Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste</b> est activé).	Vous pouvez activer ou désactiver la diffusion automatique du logiciel à l'aide de la solution System Center Configuration Manager.
<b>Lancement de la tâche</b>	Le premier lancement n'est pas défini.	La tâche Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

Tableau 57. Paramètres par défaut de la tâche Génération des règles du Contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Préfixe des noms des règles d'autorisation	Correspond au nom du serveur sur lequel Kaspersky Security for Windows Server est installé.	Vous pouvez modifier le préfixe des noms des règles d'autorisation.



Paramètre	Valeur par défaut	Description
Zone d'application des règles d'autorisation	<p>La zone d'application des règles d'autorisation reprend par défaut les catégories de fichiers suivantes :</p> <ul style="list-style-type: none"> <li>• Fichiers portant l'extension EXE et placés dans les dossiers C:\Windows, C:\Program Files (x86) et C:\Program Files ;</li> <li>• Paquets MSI, placés dans le dossier C:\Windows ;</li> <li>• Scripts placés dans le dossier C:\Windows.</li> </ul> <p>La tâche crée également des règles pour toutes les applications déjà en cours d'exécution, quels que soient leur emplacement ou leur format.</p>	<p>Vous pouvez modifier la zone de protection en ajoutant ou en supprimant des chemins d'accès aux dossiers et en définissant les types de fichiers dont le lancement sera autorisé par les règles créées automatiquement. Vous pouvez également ne pas tenir compte des applications déjà en cours d'exécution lors de la création des règles d'autorisation.</p>
Critères de génération de règles d'autorisation.	<p>Utilisation de l'en-tête et de l'empreinte du certificat numérique ; les règles sont générées pour tous les utilisateurs et groupes d'utilisateurs.</p>	<p>Vous pouvez utiliser le hash SHA256 lors de la génération de règles d'autorisation.</p> <p>Vous pouvez sélectionner l'utilisateur ou le groupe d'utilisateurs pour lesquels les règles d'autorisation doivent être générées automatiquement.</p>
Actions une fois la tâche terminée	<p>Les règles d'autorisation sont ajoutées à la liste des règles du Contrôle du lancement des applications ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont supprimés.</p>	<p>Vous pouvez ajouter des règles aux règles existantes sans fusion et sans suppression des doublons, ou remplacer les règles existantes par de nouvelles règles d'autorisation, ainsi que configurer les paramètres d'exportation des règles d'autorisation dans un fichier.</p>
Paramètres du lancement de la tâche avec autorisations	<p>La tâche est lancée sous les autorisations du compte système.</p>	<p>Vous pouvez autoriser le lancement de la tâche de Génération des règles du Contrôle du lancement des applications sous l'autorisation du compte système ou du compte d'un utilisateur que vous aurez choisi.</p>
Planification du lancement de la tâche	<p>Le premier lancement n'est pas défini.</p>	<p>La tâche Génération des règles du Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server. Vous pouvez lancer la tâche manuellement ou planifier son exécution.</p>

# Administration du Contrôle du lancement des applications via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des serveurs du réseau.

## Dans cette section

Navigation .....	<a href="#">371</a>
Configuration des paramètres de la tâche Contrôle du lancement des applications .....	<a href="#">373</a>
Configuration du contrôle de la distribution des logiciels .....	<a href="#">376</a>
Configuration de la tâche Génération des règles du Contrôle du lancement des applications .....	<a href="#">379</a>
Configuration des règles du Contrôle du lancement des applications via Kaspersky Security Center .....	<a href="#">381</a>
Création d'une tâche Génération des règles du Contrôle du lancement des applications .....	<a href="#">390</a>
Utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center .....	<a href="#">395</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications .....	<a href="#">371</a>
Accès à la liste des règles du Contrôle du lancement des applications .....	<a href="#">372</a>
Ouverture de l'assistant de la tâche Génération des règles du Contrôle du lancement des applications .....	<a href="#">372</a>

## Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications

► *Pour accéder aux paramètres de la tâche Contrôle du lancement des applications via une stratégie de Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.

6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle du lancement des applications**.  
La fenêtre **Contrôle du lancement des applications** s'ouvre.  
Configurez la stratégie en fonction des besoins.

## Accès à la liste des règles du Contrôle du lancement des applications

► *Pour accéder à la liste des règles du Contrôle du lancement des applications via Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle du lancement des applications**.  
La fenêtre **Contrôle du lancement des applications** s'ouvre.
7. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.  
La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.  
Configurez la liste des règles en fonction des besoins.

## Ouverture de l'assistant de la tâche Génération des règles du Contrôle du lancement des applications

► *Pour créer une tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Cliquez sur le bouton **Créer une tâche**.  
La fenêtre **Assistant de nouvelle tâche** s'ouvre.
5. Sélectionnez la tâche **Génération des règles du Contrôle du lancement des applications**.
6. Cliquez sur **Suivant**.  
La fenêtre **Configuration** s'ouvre.

► *Pour configurer la tâche existante Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

La fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** s'ouvre.

Consultez la section Configuration de la tâche Génération des règles du Contrôle du lancement des applications pour en savoir plus sur la configuration de la tâche.

## Configuration des paramètres de la tâche Contrôle du lancement des applications

► *Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Contrôle du lancement des applications** (cf. section "**Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications**" à la page [371](#)).
2. Sous l'onglet **Général**, sélectionnez les paramètres suivants dans la section **Mode de tâche** :
  - Dans la liste déroulante **Mode de tâche**, définissez le mode de la tâche.

La liste déroulante permet de sélectionner un des modes de la tâche Contrôle du lancement des applications :

- **Actif.** Kaspersky Security for Windows Server utilise les règles définies pour contrôler le lancement de n'importe quelle application.
- **Statistiques uniquement.** Kaspersky Security for Windows Server n'utilise pas les règles définies pour contrôler les lancements d'application. Il se contente d'enregistrer les informations relatives aux événements de lancement dans le journal d'exécution de la tâche. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles du Contrôle du lancement des applications sur la base des informations relatives aux lancements d'applications interdits qui ont été consignées dans le journal d'exécution de la tâche.

Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques uniquement**.

- Décochez ou cochez la case **Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs**.

La case active ou désactive le contrôle d'un nouveau lancement de l'application en fonction des informations d'incidents stockées dans le cache.

Quand la case est cochée, Kaspersky Security for Windows Server autorise ou interdit les lancements suivants d'une application sur la base de la conclusion de la tâche suite au premier lancement de l'application. Par exemple, si le premier lancement de l'application avait été autorisé par les règles, l'enregistrement relatif à cet événement est enregistré dans le cache et les lancements ultérieurs de cette application sont également autorisés,

sans vérification additionnelle.

Si la case est désactivée, Kaspersky Security for Windows Server analyse l'application à chacune des tentatives de lancement.

Cette case est cochée par défaut.

- Décochez ou cochez la case **Interdire le lancement de l'interpréteur de ligne de commande sans commande à exécuter**.

Si la case est cochée, Kaspersky Security for Windows Server refuse le lancer les interpréteurs de ligne de commande même si ce lancement est autorisé. Il est possible de lancer un interpréteur de ligne de commande sans commande uniquement si les deux conditions suivantes sont remplies :

- Le lancement de l'interpréteur de ligne de commande est autorisé.
- La commande à exécuter est autorisée.

Si la case est décochée, Kaspersky Security for Windows Server tient uniquement compte des règles d'autorisation pour lancer un interpréteur de ligne de commande. Le lancement est interdit si aucune règle d'autorisation n'est appliquée ou si le processus exécutable n'est pas considéré comme processus de confiance par KSN. Si une règle d'autorisation s'applique ou si KSN considère qu'il s'agit d'un processus de confiance, il est possible de lancer un interpréteur de ligne de commande avec ou sans commande à exécuter.

Kaspersky Security for Windows Server reconnaît les interpréteurs de ligne de commande suivants :

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

Cette case est décochée par défaut.

3. Dans la section **Gestion des règles**, configurez les paramètres d'application des règles :
  - a. Cliquez sur le bouton **Liste des règles** pour ajouter des règles d'autorisation de la tâche Contrôle du lancement des applications.

Kaspersky Security for Windows Server ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

- b. Sélectionnez le mode d'application des règles :
  - **Remplacer les règles locales par les règles de la stratégie.**

L'application applique la liste de règles indiquées dans la stratégie dans le cadre du contrôle centralisé du lancement des applications sur le groupe d'ordinateurs. La création, la modification ou l'application de règles locales ne sont pas disponibles.
  - **Ajouter les règles de la stratégie aux règles locales.**

L'application applique la liste de règles définie dans la stratégie en même temps que les listes de règles locales. Vous pouvez modifier les listes de règles locales à l'aide de tâches de Génération des règles du Contrôle du lancement des applications.

Par défaut Kaspersky Security for Windows Server applique deux règles prédéfinies qui autorisent l'exécution des scripts, des paquets MSI et des fichiers exécutables si ceux-ci possèdent une signature numérique de confiance.

4. Définissez les paramètres suivants dans la section **Zone d'application des règles** :

- **Utiliser les règles pour les fichiers exécutables.**

La case active ou désactive le contrôle de lancement des fichiers exécutables.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le lancement des fichiers exécutables à l'aide des règles indiquées dont les paramètres désignent les **Fichiers exécutables** comme zone d'action.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le lancement des fichiers exécutables à l'aide des règles indiquées. Le lancement des fichiers exécutables est autorisé.

Cette case est cochée par défaut.

- **Contrôle du chargement des modules DLL.**

La case active ou désactive le contrôle du chargement des modules DLL.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le chargement des modules DLL à l'aide des règles indiquées dont les paramètres incluent les **Fichiers exécutables** dans la zone d'action.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le chargement des modules DLL à l'aide des règles indiquées. Le chargement des modules DLL est autorisé.

La case est active si la case **Utiliser les règles pour les fichiers exécutables** est cochée.

Cette case est décochée par défaut.

Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation.

- **Utiliser les règles pour les scripts et les paquets MSI.**

La case active ou désactive le lancement des scripts et des paquets MSI.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le lancement des scripts et paquets MSI à l'aide des règles indiquées dont les paramètres incluent les scripts et les paquets MSI dans la zone.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le lancement des scripts et des paquets MSI à l'aide des règles indiquées. Le lancement des scripts et des paquets MSI est autorisé.

Cette case est cochée par défaut.

5. Dans la zone **Utilisation du KSN**, configurez les paramètres suivants du lancement des applications :

- **Interdire les applications douteuses selon le KSN.**

La case active ou désactive le Contrôle du lancement des applications selon les données

relatives à leur réputation dans KSN.

Si la case est cochée, Kaspersky Security for Windows Server interdit le lancement de toute application que KSN considère comme douteuse. Les règles d'autorisation du Contrôle du lancement des applications applicables aux applications considérées comme douteuses par KSN ne sont pas déclenchées. Cocher cette case permet d'assurer une protection complémentaire contre les applications malveillantes.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte la réputation des applications douteuses selon KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

- **Autoriser les applications de confiance selon le KSN.**

La case active ou désactive le Contrôle du lancement des applications selon les données relatives à leur réputation dans KSN.

Si la case est cochée, Kaspersky Security for Windows Server autorise le lancement des applications considérées comme de confiance dans le KSN. Les règles d'interdiction du Contrôle du lancement des applications qui s'appliquent aux applications de confiance dans KSN ont une priorité supérieure : si l'application est considérée comme une application de confiance par les services KSN, son lancement est interdit.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte la réputation des applications de confiance dans KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

- Utilisateurs et/ou groupes d'utilisateurs pour lesquels le lancement d'applications considérées comme des applications de confiance dans le KSN est autorisé.

6. Sous l'onglet **Contrôle de la distribution des logiciels**, configurez les paramètres du contrôle de la distribution des logiciels (cf. section "Configuration du contrôle de la distribution des logiciels" à la page [376](#)).
7. L'onglet **Administration des tâches** permet de configurer les paramètres du lancement planifié de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [138](#)).
8. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Configuration du contrôle de la distribution des logiciels

► *Pour ajouter un paquet de distribution de confiance, procédez comme suit :*

1. Ouvrez la fenêtre **Contrôle du lancement des applications** (cf. section "Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications" à la page [371](#)).
2. Sous l'onglet **Contrôle de la distribution des logiciels**, cochez la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste**.

La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide des applications et des paquets d'installation repris dans la



liste.

Si la case est cochée, l'application autorise automatiquement le lancement des fichiers exécutés à l'aide des distributions des paquets de confiance. La liste des applications et des paquets de distribution qui peuvent être lancés est modifiable.

Si la case est décochée, l'application ne tient pas compte des exclusions indiquées dans la liste.

Cette case est décochée par défaut.

Vous pouvez cocher la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** si la case **Utiliser les règles pour les fichiers exécutables** sous l'onglet **Général** est cochée dans les paramètres de la tâche **Contrôle du lancement des applications**.

3. Le cas échéant, décochez la case **Toujours autoriser la diffusion de logiciel via Windows Installer**.

La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide du sous-système Windows Installer.

Si la case est cochée, les fichiers installés via Windows Installer pourront toujours être lancés.

Si la case est décochée, le lancement sans condition des fichiers ne sera pas autorisé, même s'ils sont lancés via Windows Installer.

Cette case est cochée par défaut.

La case ne peut être modifiée si la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** n'est pas cochée.

Il est conseillé de décocher la case **Toujours autoriser la diffusion de logiciel via Windows Installer** uniquement dans les cas extrêmes. La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.

4. Le cas échéant, cochez la case **Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)**.

La case active ou désactive l'autorisation automatique de la diffusion du logiciel avec l'aide de la solution System Center Configuration Manager.

Si la case est cochée, Kaspersky Security for Windows Server autorise automatiquement le déploiement de Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de distribuer une application uniquement à l'aide du service de transfert intelligent en arrière-plan (Background Intelligent Transfer Service).

L'application contrôle le lancement des objets qui portent les extensions suivantes :

- .exe
- .msi

Cette case est décochée par défaut.



L'application contrôle le cycle de distribution de logiciels sur le serveur, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de l'application sur le serveur.

5. Pour modifier la liste des paquets de distribution de confiance, cliquez sur le bouton **Modifier la liste de paquets** et sélectionnez une des méthodes suivantes dans la fenêtre qui s'ouvre :
- **Ajouter un paquet de distribution.**
    - a. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de lancement de l'application ou le paquet d'installation.

Les données du fichier sélectionné sont ajoutées automatiquement à la section **Critères de confiance**.
    - b. Cochez ou décochez la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**.
    - c. Choisissez une de deux options proposées pour les critères de confiance qui vont déterminer si un fichier ou un paquet d'installation peut être considéré comme étant de confiance :
      - **Utiliser un certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.
      - **Utiliser le hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.
  - **Ajouter plusieurs paquets selon le hash.**

Vous pouvez choisir un nombre illimité de fichiers de lancement et de paquets d'installation et les ajouter simultanément à la liste. Kaspersky Security for Windows Server tient compte du hash et autorise le lancement le système d'exploitation à lancer les fichiers indiqués.
  - **Modifier le paquet sélectionné.**

Cette option permet de sélectionner un autre fichier de lancement ou un autre paquet d'installation. Elle

permet également la modification des critères de confiance.

- **Importer la liste des paquets de distribution depuis un fichier.**

Vous pouvez importer la liste des paquets de distribution de confiance depuis un fichier de configuration. Pour être reconnu par Kaspersky Security for Windows Server, ce fichier doit répondre aux paramètres suivants :

- Le fichier possède l'extension TXT.
- contenir des informations présentées sur la forme d'une liste de lignes contenant chacune des données pour un des fichiers de confiance ;
- contenir une liste correspondant à un des deux formats suivants :
  - <nom du fichier>:<hash SHA256>.
  - <hash SHA256>\*<nom du fichier>.

Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des distributions des paquets de confiance.

6. Si vous voulez supprimer de la liste des éléments de confiance une application ou un paquet d'installation qui avait été ajouté antérieurement, cliquez sur le bouton **Supprimer les paquets d'installation**. Le lancement des fichiers extraits sera autorisé.

Pour interdire le lancement des fichiers extraits, désinstallez l'application du serveur protégé ou créez une règle d'interdiction dans les paramètres de la tâche **Contrôle du lancement des applications**.

7. Cliquez sur le bouton **OK**.

Les nouvelles valeurs des paramètres seront enregistrés.

## Configuration de la tâche **Génération des règles du Contrôle du lancement des applications**

► *Pour configurer la tâche **Génération des règles du Contrôle du lancement des applications**, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** (cf. section "**Ouverture de l'Assistant de tâche Génération des règles du Contrôle du lancement des applications e des propriétés**" à la page [372](#)).
2. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

3. La section **Configuration** permet de configurer les paramètres suivants :
  - Ajoutez un préfixe pour les noms des règles.
  - Configurez la zone d'application des règles d'autorisation :
    - Créer des règles d'autorisation sur la base des applications en cours d'exécution ;
    - Créer des règles d'autorisation pour les applications de dossiers spécifiques.
4. Vous pouvez indiquer les actions à réaliser lors de la création des règles d'autorisation du Contrôle du

lancement des applications dans la section **Options** :

- **Utiliser un certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.

- **Utiliser l'objet et l'empreinte du certificat numérique**

La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique.

Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications. Kaspersky Security for Windows Server autorise désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique désignés.

L'utilisation de cette case limite fortement le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée.

Si la case est désélectionnée, un critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation.

La case est active si vous avez choisi l'option **Utiliser un certificat numérique**.

Cette case est cochée par défaut.

- **En cas d'absence de certificat, utiliser**

Il s'agit d'une liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le Contrôle du lancement des applications dans le cas où le fichier utiliser pour créer la règle ne dispose pas d'un certificat numérique.

- **hash SHA256.** La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
  - **chemin du fichier.** Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.
  - **Utiliser le hash SHA256**
- Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application

autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Créer des règles pour un utilisateur ou un groupe d'utilisateurs.**

Il s'agit d'un champ qui affiche un utilisateur ou un groupe d'utilisateurs. L'application contrôlera toutes les applications exécutées par l'utilisateur ou le groupe d'utilisateurs défini.

Par défaut, le groupe **Tous** est sélectionné.

Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security for Windows Server crée à la fin des tâches.

5. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
6. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
7. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

*Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le [Système d'aide de Kaspersky Security Center](#).*

8. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

## Configuration des règles du Contrôle du lancement des applications via Kaspersky Security Center

Apprenez à créer une liste de règles sur la base de différents critères ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle du lancement des applications.

## Dans cette section

Ajout d'une règle de contrôle du lancement des applications .....	<a href="#">382</a>
Activation du mode Autoriser par défaut .....	<a href="#">385</a>
Création de règles d'autorisation au départ d'événements de Kaspersky Security Center .....	<a href="#">385</a>
Importation des règles depuis un rapport de Kaspersky Security Center sur les applications bloquées.....	<a href="#">386</a>
Importation des règles du Contrôle du lancement des applications depuis un fichier XML .....	<a href="#">388</a>
Vérification du lancement des applications .....	<a href="#">390</a>

## Ajout d'une règle de contrôle du lancement des applications

► *Pour ajouter une règle de contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications** (cf. section "Accès à la liste des règles du Contrôle du lancement des applications" à la page [372](#)).
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.  
La fenêtre **Paramètres de règle** s'ouvre.
4. Spécifiez les paramètres suivants :
  - a. Dans le champ **Nom**, saisissez le nom de la règle.
  - b. Dans la liste déroulante **Type**, sélectionnez le type de règle :
    - **Autorisé**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
    - **Interdit**, si vous souhaitez que la règle interdise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
  - c. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
    - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
    - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
  - d. Dans le champ **Utilisateur ou groupe d'utilisateurs**, indiquez les utilisateurs qui pourront ou non lancer des applications en fonction du type de règle. Pour ce faire, procédez comme suit :
    - i. Cliquez sur le bouton **Parcourir**.
    - ii. La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.
    - iii. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.
    - iv. Cliquez sur le bouton **OK**.
  - e. Réalisez les opérations suivantes si vous souhaitez extraire les valeurs pour les critères de déclenchement de la règle listés dans la section **Critères de déclenchement de la règle**, depuis un

fichier :

- i. Cliquez sur le bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**.

La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

- ii. Sélectionnez le fichier.
- iii. Cliquez sur le bouton **Ouvrir**.

Les valeurs des critères dans le fichier sont affichées dans les champs de la section **Critères de déclenchement de la règle**. Par défaut, c'est le premier critère de la liste dont les données figurent dans les propriétés du fichier qui est sélectionné.

- f. Dans la section **Critères de déclenchement de la règle**, sélectionnez une des options suivantes :

- **Certificat numérique**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique :
  - Cochez la case **Utiliser l'objet**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'en-tête indiqué.
  - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle uniquement le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'empreinte indiquée.
- **Hash SHA256**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers dont la somme de contrôle correspond à celle indiquée.
- **Chemin du fichier**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.

Kaspersky Security for Windows Server ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

- g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :

- i. Dans la section **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

La fenêtre **Exclusion de la règle** s'ouvre.

- ii. Dans le champ **Nom**, saisissez le nom de l'exclusion.
- iii. Indiquez les paramètres d'exclusions des fichiers des applications de la règle de contrôle du lancement des applications. Vous pouvez remplir les champs des paramètres depuis les propriétés du fichier en cliquant sur le bouton **Définir l'exclusion selon les propriétés du fichier**.

- **Certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.

- **Utiliser l'objet**

La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que

critère de déclenchement de la règle.

Si la case est cochée, l'objet du certificat numérique indiqué sera utilisé en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications uniquement pour l'éditeur repris dans l'en-tête.

Si la case est décochée, l'application n'utilise pas les en-têtes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, la règle créée contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quel en-tête.

L'en-tête du certificat numérique utilisé pour signer le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**

La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de déclenchement de la règle.

Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications signées par le certificat numérique doté de l'empreinte indiquée.

Si la case est décochée, l'application n'utilise pas l'empreinte de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, l'application contrôlera le lancement des applications signées à l'aide du certificat numérique doté n'importe quelle empreinte.

L'empreinte du certificat numérique utilisé pour signer le fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Chemin du fichier**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas



pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.

- iv. Cliquez sur le bouton **OK**.
- v. Si nécessaire, répétez les étapes (i) à (iv) pour ajouter des exclusions supplémentaires.

5. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

## Activation du mode Autoriser par défaut

La règle Autoriser par défaut autorise le lancement de toutes les applications si celui-ci n'est pas interdit par des règles ou par une conclusion de KSN qui les considère comme douteuses. Il est possible d'activer le mode Autoriser par défaut en ajoutant des règles d'autorisation spécifiques. Vous pouvez activer Autoriser par défaut uniquement pour les scripts ou pour tous les fichiers exécutables.

► *Pour ajouter une nouvelle règle Autoriser par défaut :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications** (cf. section "**Accès à la liste des règles du Contrôle du lancement des applications**" à la page [372](#)).
2. Cliquez sur le bouton **Ajouter** et, dans le menu contextuel du bouton, sélectionnez **Ajouter une règle**.  
La fenêtre **Paramètres de règle** s'ouvre.
3. Dans le champ **Nom**, saisissez le nom de la règle.
4. Dans la liste déroulante **Type**, sélectionnez le type de règle **Autorisé** :
5. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
  - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
  - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
6. Dans la section **Critères de déclenchement de la règle**, sélectionnez l'option **Chemin du fichier**.
7. Saisissez le masque suivant : ? : \
8. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique le mode Autoriser par défaut.

## Création de règles d'autorisation au départ d'événements de Kaspersky Security Center

► *Afin de créer des règles d'autorisation pour les applications au départ des événements de Kaspersky Security Center dans le Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications** (cf. section "**Accès à la liste des règles du Contrôle du lancement des applications**" à la page [372](#)).
2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Créer des règles d'autorisation des applications à partir des événements de Kaspersky Security Center**.
3. Sélectionnez le principe d'ajout des règles à la liste des règles du Contrôle du lancement des applications



déjà créées :

- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

La fenêtre **Création de règles du Contrôle du lancement des applications** s'ouvre.

4. Définissez les paramètres de requête suivants :
  - **Adresse du Serveur d'administration**
  - **Port**
  - **Utilisateur**
  - **Mot de passe**
5. Sélectionnez les types d'événements qui vont être utilisé par la tâche de création de règle :
  - **mode Statistiques uniquement : lancement de l'application interdit.**
  - **Lancement de l'application interdit.**
6. Sélectionnez la période dans la liste déroulante **Événements de requête générés au cours de la période.**
7. Cliquez sur le bouton **Créer des règles.**
8. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du contrôle du lancement des applications.**

La liste des règles dans la stratégie Contrôle du lancement des applications est enrichie de nouvelles règles formées sur la base des données du système du serveur sur lequel la Console d'administration Kaspersky Security Center est installée.

Si la liste des règles du Contrôle du lancement des applications est déjà définie dans la stratégie, Kaspersky Security for Windows Server ajoute les règles choisies parmi les événements du verrouillage aux règles déjà définies. Les règles possédant le même hash ne sont pas ajoutées car toutes les règles d'une liste doivent être uniques.

## Importation des règles depuis un rapport de Kaspersky Security Center sur les applications bloquées

Vous pouvez importer les données relatives aux lancements d'application bloqués depuis le rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche Contrôle du lancement des applications en mode **Statistiques uniquement** et appliquer ces données à la composition d'une liste de règles d'autorisation du Contrôle du lancement d'applications dans la stratégie configurée.

Lors de la création d'un rapport sur les événements survenus pendant l'exécution de la tâche de Contrôle du lancement des applications, vous pouvez surveiller le lancement des applications qu'il faudra bloquer.

Lors de l'importation depuis un rapport des données sur les applications bloquées dans les paramètres de la stratégie, confirmez que la liste à utiliser contient uniquement les applications dont vous souhaitez autoriser le lancement.

► Pour définir les règles d'autorisation du Contrôle du lancement des applications pour un groupe de serveurs sur la base du rapport des applications bloquées de Kaspersky Security Center :

1. Ouvrez la fenêtre **Contrôle du lancement des applications** (cf. section "Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications" à la page [371](#)).
2. Dans la section **Mode de tâche**, sélectionnez le mode **Statistiques uniquement**.
3. Dans la section **Notifications sur les événements** des propriétés de la stratégie, assurez-vous que :
  - S'agissant des **Événements critiques**, la durée de conservation du journal d'exécution de la tâche pour les événements **Lancement de l'application interdit** est supérieure à la période prévue d'exécution de la tâche en mode **Statistiques uniquement** (30 jours est la valeur par défaut).
  - S'agissant des événements qui possèdent le niveau d'importance **Avertissement**, la durée de conservation du journal d'exécution de la tâche pour les événements **mode Statistiques uniquement : lancement de l'application interdit** est supérieure à la période prévue d'exécution de la tâche en mode **Statistiques uniquement** (30 jours est la valeur par défaut).

A l'issue de la période de conservation des événements, les informations relatives aux événements enregistrés sont supprimées et ne figurent pas dans le fichier du rapport. Avant de lancer la tâche Contrôle du lancement des applications en mode **Statistiques uniquement**, assurez-vous que la durée d'exécution de la tâche n'est pas supérieure à la période configurée pour les événements indiqués.

4. Une fois la tâche terminée, exportez les événements enregistrés dans un fichier .TXT :
  - a. Dans l'espace de travail du nœud **Serveur d'administration** de Kaspersky Security Center, sélectionnez l'onglet **Événements**.
  - b. Cliquez sur le bouton **Créer une sélection** pour créer une sélection d'événements sur la base de la caractéristique *Bloqués* afin de voir les applications dont le lancement sera bloqué par la tâche de Contrôle du lancement des applications.
  - c. Dans le panneau de détails de la sélection, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites dans un fichier au format TXT.

Avant d'importer et d'appliquer un rapport créé dans une stratégie, assurez-vous qu'il contient uniquement les données relatives aux applications dont vous souhaitez autoriser le lancement.

5. Importez les données relatives aux lancements d'application bloqués dans la tâche de Contrôle du lancement des applications. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie, dans les paramètres de la tâche Contrôle du lancement des applications :
  - a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.  
La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.
  - b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Importer les données relatives aux applications bloquées depuis le rapport de Kaspersky Security Center**.

- c. Sélectionnez le principe d'ajout des règles depuis la liste créée sur la base d'un rapport de Kaspersky Security Center à la liste des règles du Contrôle du lancement des applications existantes :
- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
  - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
  - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.
- d. Dans la fenêtre Microsoft Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les lancements d'application bloqués ont été exportés.
- e. Cliquez sur le bouton **OK** dans la fenêtre Règles du contrôle du lancement des applications et dans la fenêtre **Paramètres de la tâche**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les applications bloquées seront ajoutées à la liste des règles du Contrôle du lancement des applications.

## Importation des règles du Contrôle du lancement des applications depuis un fichier XML

Vous pouvez importer les rapports créés par la tâche de groupe Génération des règles du Contrôle du lancement des applications et les appliquer en guise de liste de règles d'autorisation dans la stratégie configurée.

A la fin de la tâche de groupe de Génération des règles du Contrôle du lancement des applications, l'application exporte les règles d'autorisation créées dans un fichier au format XML enregistré dans le dossier partagé indiqué. Chaque fichier contenant une liste de règles est créé en analysant les fichiers exécutés et les applications lancées sur chaque serveur distinct du réseau de l'organisation. Les listes contiennent les règles d'autorisation du lancement pour les fichiers et les applications dont le type correspond au type repris dans les paramètres de la tâche de groupe Génération des règles du Contrôle du lancement des applications.

► *Pour définir les règles d'autorisation du Contrôle du lancement des applications pour un groupe de serveurs sur la base d'une liste de règles d'autorisation créées automatiquement, procédez comme suit :*

1. Sous l'onglet **Tâches** dans le panneau d'administration du groupe de serveur configuré, créez une tâche de groupe Génération des règles du Contrôle du lancement des applications ou choisissez une tâche existante (cf. section "Accès à la génération de règles pour l'assistant de la tâche Génération des règles du Contrôle du lancement des applications et aux propriétés" à la page [372](#)).
2. Dans les propriétés de la tâche de groupe de Génération des règles du Contrôle du lancement des applications créée ou dans l'Assistant de création de tâche, configurez les paramètres suivants :
  - Dans la section **Notification**, configurez les paramètres de conservation du rapport sur l'exécution de la tâche.

Les détails sur la configuration des paramètres de cette section sont repris dans l'aide de Kaspersky Security Center.

- Dans la section **Configuration**, indiquez les types d'applications dont le lancement sera autorisé par les règles créées. Vous pouvez également modifier la sélection de dossiers contenant les applications qui pourront être lancées : exclure les dossiers indiqués par défaut de la zone d'application de la tâche et

ajouter manuellement de nouveaux dossiers.

- Dans la section **Options**, indiquez les actions de la tâche pendant son exécution et à son issue. Définissez le critère de génération de règle et le nom du fichier dans lequel les règles créées vont être exportées.
- Dans la section **Planification**, configurez les paramètres de planification du lancement de la tâche.
- Dans la section **Compte**, désignez le compte utilisateur sous les privilèges duquel la tâche sera exécutée.
- Dans la section **Exclusions de la zone de la tâche**, définissez les groupes de serveurs qu'il faut exclure de la zone d'action de la tâche.

Kaspersky Security for Windows Server ne crée pas de règles d'autorisation pour les applications lancées sur les serveurs exclus.

3. Sous l'onglet **Tâches** du panneau d'administration du groupe de serveurs configurés, sélectionnez la Génération des règles du Contrôle du lancement des applications créée dans la liste des tâches de groupe, puis cliquez sur le bouton **Démarrer** pour lancer la tâche.

Quand la tâche est finie, les listes de règles d'autorisation générées automatiquement sont enregistrées dans un fichier XML au sein d'un dossier partagé.

Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier partagé n'est pas prévue par la stratégie de l'organisation, nous vous conseillons de lancer la tâche Génération des règles du Contrôle du lancement des applications sur un serveur appartenant au groupe de serveurs d'essai ou sur une machine modèle.

4. Pour ajouter les listes de règles d'autorisation créées à la tâche de Contrôle du lancement des applications, procédez comme suit :
  - a. Ouvrez la fenêtre **Règles du Contrôle du lancement des applications** (cf. section "Accès à la liste des règles du Contrôle du lancement des applications" à la page [372](#)).
  - b. Cliquez sur le bouton **Ajouter** et dans la liste qui s'ouvre, choisissez l'option **Importer les règles depuis un fichier au format XML**.
  - c. Sélectionnez le principe d'ajout des règles d'autorisation générées automatiquement à la liste des règles du Contrôle du lancement des applications déjà créées :
    - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
    - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
    - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.
  - d. Dans la fenêtre Microsoft Windows standard qui s'ouvre, choisissez les fichiers au format XML créés à l'issue de la tâche de groupe Génération des règles du Contrôle du lancement des applications.
  - e. Cliquez sur le bouton **OK** dans la fenêtre **Règles du contrôle du lancement des applications** et dans la fenêtre **Paramètres de la tâche**.

5. Si vous souhaitez appliquer les règles créées pour contrôler le lancement des applications, sélectionnez le mode **Actif** pour la tâche dans les propriétés de la tâche Contrôle du lancement des applications dans la stratégie.

Les règles d'autorisation générées automatiquement sur la base des lancements de tâches sur chaque serveur distinct seront appliquées à tous les serveurs du réseau soumis à la stratégie configurée. Pour ces serveurs, l'application autorise le lancement uniquement des applications pour lesquelles des règles d'autorisation ont été créées.

## Vérification du lancement des applications

Avant d'appliquer les règles configurées du Contrôle du lancement des applications, vous pouvez tester n'importe quelle application afin d'identifier les règles du Contrôle du lancement des applications déclenchées par cette application.

Kaspersky Security for Windows Server bloque par défaut le lancement des applications si celui-ci n'est autorisé par aucune règle. Pour éviter l'interdiction du lancement d'applications importantes, il faut créer des règles d'autorisation pour celles-ci.

Si le lancement de l'application est régi par plusieurs règles de différents types, les règles d'interdiction sont prioritaires : le lancement de l'application est interdit si celle-ci tombe sous le coup d'une seule règle d'interdiction.

► *Pour tester les règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications** (cf. section "Accès à la liste des règles du Contrôle du lancement des applications" à la page [372](#)).
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Afficher les règles pour le fichier**.  
La fenêtre standard de Microsoft Windows s'ouvre.
3. Sélectionnez le fichier pour lequel vous souhaitez tester la règle de contrôle.

Le chemin d'accès au fichier indiqué apparaît dans la ligne de recherche. La liste contient toutes les règles qui vont être déclenchées au lancement du fichier sélectionné.

## Création d'une tâche Génération des règles du Contrôle du lancement des applications

► *Pour créer une tâche Génération des règles du contrôle du lancement des applications et configurer ses paramètres, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration** dans l'Assistant Nouvelle tâche (cf. section "Accès à la génération de règles pour l'assistant de la tâche Génération des règles du Contrôle du lancement des applications et aux propriétés" à la page [372](#)).
2. Configurez les éléments suivants :
  - Indiquez le **Préfixe pour les noms des règles**.

Il s'agit de la première partie du nom de la règle. La deuxième partie du nom de la règle est constituée à partir du nom de l'objet dont le lancement est autorisé.

Par défaut, le nom du serveur sur lequel est installé Kaspersky Security for Windows Server est utilisé comme préfixe. Vous pouvez modifier le préfixe des noms des règles d'autorisation.

- Configurez la zone d'application des règles d'autorisation (cf. Section "Restriction de la zone d'application de la tâche" à la page [411](#)).
3. Cliquez sur **Suivant**.
  4. Définissez les actions que Kaspersky Security for Windows Server doit réaliser :
    - Lors de la génération de règles d'autorisation (cf. section "Actions à réaliser lors de la génération automatique de règles" à la page [412](#)).
    - Une fois la tâche terminée (cf. section "Actions à réaliser à la fin de la génération automatique de règles" à la page [413](#)).
  5. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.
  6. Cliquez sur **Suivant**.
  7. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.
  8. Cliquez sur **Suivant**.
  9. Définissez un nom de tâche.
  10. Cliquez sur **Suivant**.

Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants :  
 " \* < > & \ : |

La fenêtre **Fin de la création de la tâche** s'ouvre.

11. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.
12. Cliquez sur **Terminer** pour terminer la création de la tâche.

► *Pour configurer une règle existante dans Kaspersky Security Center, procédez comme suit :*

Ouvrez la fenêtre Propriétés : Génération des règles du Contrôle du lancement des applications et ajustez les paramètres décrits ci-dessus.

Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Dans cette section

Restriction de la zone d'application de la tâche .....	<a href="#">391</a>
Actions à réaliser lors de la génération automatique de règles.....	<a href="#">392</a>
Actions à réaliser à la fin de la génération automatique de règles.....	<a href="#">394</a>

## Restriction de la zone d'application de la tâche

► *Pour limiter la zone d'application de la tâche Génération des règles du Contrôle du lancement des*

applications, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** (cf. section "Accès à la génération de règles pour l'assistant de la tâche Génération des règles du Contrôle du lancement des applications et aux propriétés" à la page [372](#)).
2. Configurez les paramètres de la tâche suivants :

- **Créer des règles d'autorisation sur la base des applications en cours d'exécution.**

Cette case active ou désactive la création de règles du Contrôle du lancement des applications pour les applications déjà en cours d'exécution. Cette option est recommandée si une sélection d'applications de référence est en cours d'exécution sur le serveur et que vous souhaitez utiliser celle-ci pour générer les règles d'autorisation.

Si la case est cochée, les règles d'autorisation pour le contrôle du lancement des applications sont créées sur la base des applications exécutées.

Si la case est décochée, les applications en cours d'exécution ne sont pas prises en compte pour la génération des règles d'autorisation.

Cette case est cochée par défaut.

La case ne peut être décochée si aucun dossier n'est sélectionné dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**.

- **Créer des règles d'autorisation pour les applications des dossiers.**

Le tableau permet de sélectionner ou d'indiquer les dossiers pour la tâche et les types de fichiers exécutables qui seront pris en compte lors de la génération des règles du Contrôle du lancement des applications. La tâche générera des règles d'autorisation pour les fichiers des types sélectionnés et situés dans les dossiers indiqués.

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Actions à réaliser lors de la génération automatique de règles

► *Pour configurer les actions que Kaspersky Security for Windows Server doit réaliser pendant l'exécution de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** (cf. section "**Ouverture de l'Assistant de tâche Génération des règles du Contrôle du lancement des applications e des propriétés**" à la page [372](#)).
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Lors de la génération des règles d'autorisation** :

- **Utiliser un certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.



Cette option est sélectionnée par défaut.

- **Utiliser l'objet et l'empreinte du certificat numérique**

La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique.

Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications. Kaspersky Security for Windows Server autorise désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique désignés.

L'utilisation de cette case limite fortement le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée.

Si la case est désélectionnée, un critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation.

La case est active si vous avez choisi l'option **Utiliser un certificat numérique**.

Cette case est cochée par défaut.

- **En cas d'absence de certificat, utiliser**

Il s'agit d'une liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le Contrôle du lancement des applications dans le cas où le fichier utiliser pour créer la règle ne dispose pas d'un certificat numérique.

- **hash SHA256.** La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
- **chemin du fichier.** Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.

- **Utiliser le hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Créer des règles pour un utilisateur ou un groupe d'utilisateurs.**



Il s'agit d'un champ qui affiche un utilisateur ou un groupe d'utilisateurs. L'application contrôlera toutes les applications exécutées par l'utilisateur ou le groupe d'utilisateurs défini.

Par défaut, le groupe **Tous** est sélectionné.

4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Actions à réaliser à la fin de la génération automatique de règles

► *Pour configurer les actions que Kaspersky Security for Windows Server doit réaliser à la fin de la Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** (cf. section "Accès à la génération de règles pour l'assistant de la tâche Génération des règles du Contrôle du lancement des applications et aux propriétés" à la page [372](#)).
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Une fois la tâche terminée** :

- **Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications.**

La case active ou désactive l'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications. La liste des règles du Contrôle du lancement des applications est affichée via le lien **Règles du contrôle du lancement des applications** du panneau de détails du nœud Contrôle du lancement des applications.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les règles créées par la tâche Génération des règles du Contrôle du lancement des applications à la liste des règles du Contrôle du lancement des applications conformément au principe d'ajout défini.

Si la case est décochée, Kaspersky Security for Windows Server n'ajoute pas les règles d'autorisation créées à la liste de règles du Contrôle du lancement des applications. Les règles créées sont exportées uniquement dans un fichier.

Cette case est cochée par défaut.

- **Principe d'ajout.**

Il s'agit d'une liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications.

- **Ajouter aux règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes.** Les règles remplacent les règles existantes.
- **Fusionner avec les règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

Le mode **Fusionner avec les règles existantes** est sélectionné par défaut.

- **Exporter les règles d'autorisation vers un fichier.**
- **Ajouter des informations sur l'ordinateur dans le nom du fichier.**

La case active ou désactive l'ajout des informations relatives au serveur protégé au nom du fichier dans lequel sont exportées les règles d'autorisation du Contrôle des périphériques

Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur protégé ainsi que la date et l'heure de création du fichier.

Si la case est décochée, l'application n'ajoute pas les informations relatives au serveur protégé dans le nom du fichier d'exportation.

Cette case est cochée par défaut.

4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Utilisation d'un profil pour configurer les tâches Contrôle du lancement des applications dans une stratégie de Kaspersky Security Center

Les règles du Contrôle du lancement des applications, configurées dans une stratégie, s'appliquent à tous les serveurs d'un groupe d'administration. Si des serveurs de différents types ont été ajoutés à un groupe d'administration, il faudra peut-être prévoir des listes individuelles de règles pour le Contrôle du lancement des applications sur chacun d'entre eux. Pour pouvoir restreindre l'application d'une stratégie aux serveurs d'un groupe d'administration, vous pouvez utiliser des *profils de stratégie*.

Nous conseillons d'appliquer les profils de stratégie pour la configuration des règles du Contrôle du lancement des applications sur des serveurs de différents types à l'intérieur d'un même groupe d'administration géré par une seule stratégie. Ceci permet d'optimiser la protection du serveur car les règles indiquées couvrent uniquement les applications lancées généralement sur un type de serveur en particulier.

Les profils de stratégie sont appliqués à tous les serveurs du groupe d'administration conformément aux *tags* attribués à ceux-ci. Vous pouvez configurer un profil de stratégie pour tous les serveurs d'un groupe d'administration qui possèdent le même tag.

Pour en savoir plus sur les tags et les profils de stratégie et pour obtenir les instructions sur leur utilisation, consultez le *Système d'aide de Kaspersky Security Center*.

► *Pour appliquer un profil de stratégie dans la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**. Développez le groupe d'administration pour lequel vous souhaitez configurer l'application de profils de stratégie.
2. Attribuez des tags en fonction du type de serveur à chaque serveur au sein du groupe d'administration :
  - a. Dans le panneau de détails du groupe d'administration sélectionné, ouvrez l'onglet **Périphériques**.
  - b. Sélectionnez les serveurs auxquels vous souhaitez attribuer les tags.
  - c. Dans la fenêtre **Propriétés : <Nom du serveur>** du serveur sélectionné, ouvrez la section **Tags** et composez la liste des tags.
  - d. Cliquez sur le bouton **OK**.
3. Créez un profil de stratégie :
  - a. Dans le panneau de détails du groupe d'administration sélectionné, ouvrez l'onglet **Stratégies**.
  - b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer l'application de profils.

- c. Dans la fenêtre **Propriétés : <nom de la stratégie>** de la stratégie sélectionnée, ouvrez la section **Profils de la stratégie**, puis cliquez sur le bouton **Ajouter** pour créer un autre profil.  
La fenêtre **Propriétés : <nom du profil>** s'ouvre.
  4. Configurez la stratégie de protection des serveurs au sein du groupe d'administration :
    - a. Dans la section **Règles d'activation**, configurez la zone d'application du profil et définissez les conditions dans lesquelles le profil sera activé.
    - b. Dans la section **Contrôle du lancement des applications**, configurez la liste des règles du Contrôle du lancement des applications pour le profil modifié.
    - c. Cliquez sur le bouton **OK**.
  5. Dans la fenêtre **Propriétés : <nom de la stratégie>**, cliquez sur **OK**.
- Le profil configuré sera appliqué dans la stratégie pour la tâche Contrôle du lancement des applications.

## Administration du Contrôle du lancement des applications via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un serveur local.

### Dans cette section

Navigation .....	<a href="#">396</a>
Configuration des paramètres de la tâche Contrôle du lancement des applications .....	<a href="#">397</a>
Configuration des règles du Contrôle du lancement des applications .....	<a href="#">404</a>
Configuration d'une tâche Génération des règles du Contrôle du lancement des applications .....	<a href="#">410</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Accès aux paramètres de la tâche Contrôle du lancement des applications .....	<a href="#">396</a>
Ouverture de la fenêtre des règles du Contrôle du lancement des applications.....	<a href="#">397</a>
Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications .....	<a href="#">397</a>

## Accès aux paramètres de la tâche Contrôle du lancement des applications

- *Pour accéder aux paramètres généraux de la tâche Contrôle du lancement des applications via la*

*Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Contrôle du lancement des applications**.
3. Dans le panneau de détails du nœud enfant **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

## Ouverture de la fenêtre des règles du Contrôle du lancement des applications

► *Pour accéder à la liste des règles de contrôle du lancement des applications via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Contrôle du lancement des applications**.
3. Dans le panneau de détails du nœud **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

4. Configurez la liste des règles en fonction des besoins.

## Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications

► *Pour configurer la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Sélectionnez le nœud enfant **Génération des règles du Contrôle du lancement des applications**.
3. Dans le panneau de détails du nœud enfant **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

4. Configurez la tâche en fonction des besoins.

## Configuration des paramètres de la tâche Contrôle du lancement des applications

► *Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "Accès aux paramètres de la tâche Contrôle du lancement des applications" à la page [396](#)).
2. Configurez les paramètres de la tâche suivants :

- Sous l'onglet **Général** :
  - Mode de la tâche du Contrôle du lancement des applications (cf. section "Sélection du mode de la tâche Contrôle du lancement des applications" à la page [398](#)).
  - Zone d'application des règles dans la tâche (cf. section "Configuration de la zone d'application de la tâche Contrôle du lancement des applications" à la page [400](#)).
  - Utilisation du KSN (cf. section "Configuration de l'utilisation du KSN" à la page [401](#)).
  - Paramètres du Contrôle de la distribution des logiciels (cf. section "Contrôle de la distribution des logiciels" à la page [402](#)) sous l'onglet **Contrôle de la distribution des logiciels**.
  - Paramètres de planification du lancement des tâches (cf. section "Paramètres de configuration de la planification du lancement de la tâche" à la page [158](#)) sous les onglets **Planification** et **Avancé**.
- 3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.  
Les modifications apportées aux paramètres seront enregistrées.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Dans cette section

Sélection du mode de la tâche Contrôle du lancement des applications .....	<a href="#">398</a>
Configuration de la zone d'application de la tâche Contrôle du lancement des applications .....	<a href="#">400</a>
Configuration de l'utilisation du KSN .....	<a href="#">401</a>
Contrôle de la distribution des logiciels .....	<a href="#">402</a>

## Sélection du mode de la tâche Contrôle du lancement des applications

► *Pour configurer le mode de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Contrôle du lancement des applications**" à la page [396](#)).
2. Désignez le mode de la tâche dans la liste déroulante **Mode de tâche** sous l'onglet **Général**.

La liste déroulante vous permet de sélectionner un des modes d'exécution de la tâche Contrôle du lancement des applications :

- **Actif**. Kaspersky Security for Windows Server utilise les règles définies pour contrôler le lancement de n'importe quelle application exécutée.
- **Statistiques uniquement**. Kaspersky Security for Windows Server n'utilise pas les règles définies pour contrôler les lancements d'application. Il se contente d'enregistrer les informations relatives à ces lancements dans le journal d'exécution de la tâche. Le lancement de tous les programmes est autorisé. Vous pouvez utiliser ce mode pour créer une liste de règles du Contrôle du lancement des applications sur la base des informations consignées dans le journal d'exécution de la tâche.

Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques uniquement**.

3. Décochez ou cochez la case **Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs**.

La case active ou désactive le contrôle d'un nouveau lancement de l'application en fonction des informations d'incidents stockées dans le cache.

Quand la case est cochée, Kaspersky Security for Windows Server autorise ou interdit les lancements suivants d'une application sur la base de la conclusion de la tâche suite au premier lancement de l'application. Par exemple, si le premier lancement de l'application avait été autorisé par les règles, l'enregistrement relatif à cet événement est enregistré dans le cache et les lancements ultérieurs de cette application sont également autorisés, sans vérification additionnelle.

Si la case est désactivée, Kaspersky Security for Windows Server analyse l'application à chacune des tentatives de lancement.

Cette case est cochée par défaut.

Kaspersky Security for Windows Server dresse une nouvelle liste d'événements dans le cache à chaque modification des paramètres de la tâche **Contrôle du lancement des applications**. Cela signifie que le **Contrôle du lancement des applications** est organisé selon les paramètres de sécurité en cours.

4. Cochez ou décochez la case **Interdire le lancement de l'interpréteur de ligne de commande sans commande à exécuter**.

Si la case est cochée, Kaspersky Security for Windows Server refuse de lancer les interpréteurs de ligne de commande même si ce lancement est autorisé. Il est possible de lancer un interpréteur de ligne de commande sans commande uniquement si les deux conditions suivantes sont remplies :

- Le lancement de l'interpréteur de ligne de commande est autorisé.
- La commande à exécuter est autorisée.

Si la case est décochée, Kaspersky Security for Windows Server tient uniquement compte des règles d'autorisation pour lancer un interpréteur de ligne de commande. Le lancement est interdit si aucune règle d'autorisation n'est appliquée ou si le processus exécutable n'est pas considéré comme processus de confiance par KSN. Si une règle d'autorisation s'applique ou si KSN considère qu'il s'agit d'un processus de confiance, il est possible de lancer un interpréteur de ligne de commande avec ou sans commande à exécuter.

Kaspersky Security for Windows Server reconnaît les interpréteurs de ligne de commande suivants :

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

Cette case est décochée par défaut.

5. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution de la tâche.

## Configuration de la zone d'application de la tâche Contrôle du lancement des applications

► Pour définir la zone d'application de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Contrôle du lancement des applications**" à la page [396](#)).
2. Définissez les paramètres suivants dans la section **Zone d'application des règles** de l'onglet **Général** :

- **Utiliser les règles pour les fichiers exécutables**

La case active ou désactive le contrôle de lancement des fichiers exécutables.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le lancement des fichiers exécutables à l'aide des règles indiquées dont les paramètres désignent les **Fichiers exécutables** comme zone d'action.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le lancement des fichiers exécutables à l'aide des règles indiquées. Le lancement des fichiers exécutables est autorisé.

Cette case est cochée par défaut.

- **Contrôle du chargement des modules DLL**

La case active ou désactive le contrôle du chargement des modules DLL.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le chargement des modules DLL à l'aide des règles indiquées dont les paramètres incluent les **Fichiers exécutables** dans la zone d'action.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le chargement des modules DLL à l'aide des règles indiquées. Le chargement des modules DLL est autorisé.

La case est active si la case **Utiliser les règles pour les fichiers exécutables** est cochée.

Cette case est décochée par défaut.

Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation.

- **Utiliser les règles pour les scripts et les paquets MSI**

La case active ou désactive le lancement des scripts et des paquets MSI.

Si la case est cochée, Kaspersky Security for Windows Server autorise ou interdit le lancement des scripts et paquets MSI à l'aide des règles indiquées dont les paramètres incluent les scripts et les paquets MSI dans la zone.

Si la case est décochée, Kaspersky Security for Windows Server ne contrôle pas le lancement des scripts et des paquets MSI à l'aide des règles indiquées. Le lancement des scripts et des paquets MSI est autorisé.

Cette case est cochée par défaut.

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.



## Configuration de l'utilisation du KSN

► Pour configurer l'utilisation des services KSN pour la tâche *Contrôle du lancement des applications*, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Contrôle du lancement des applications**" à la page [396](#)).
2. Sous l'onglet **Général**, dans la section **Utilisation du KSN**, définissez les paramètres relatifs à l'utilisation des services du KSN :

- Le cas échéant, cochez la case **Interdire les applications douteuses selon le KSN**.

La case active ou désactive le Contrôle du lancement des applications selon les données relatives à leur réputation dans KSN.

Si la case est cochée, Kaspersky Security for Windows Server interdit le lancement de toute application que KSN considère comme douteuse. Les règles d'autorisation du Contrôle du lancement des applications applicables aux applications considérées comme douteuses par KSN ne sont pas déclenchées. Cocher cette case permet d'assurer une protection complémentaire contre les applications malveillantes.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte la réputation des applications douteuses selon KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

- Le cas échéant, cochez la case **Autoriser les applications de confiance selon le KSN**.

La case active ou désactive le Contrôle du lancement des applications selon les données relatives à leur réputation dans KSN.

Si la case est cochée, Kaspersky Security for Windows Server autorise le lancement des applications considérées comme de confiance dans le KSN. Les règles d'interdiction du Contrôle du lancement des applications qui s'appliquent aux applications de confiance dans KSN ont une priorité supérieure : si l'application est considérée comme une application de confiance par les services KSN, son lancement est interdit.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte la réputation des applications de confiance dans KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

- Si la case **Autoriser les applications de confiance selon le KSN** est cochée, indiquez les utilisateurs et/ou les groupes d'utilisateurs qui peuvent lancer les applications considérées comme des applications de confiance dans KSN. Pour ce faire, procédez comme suit :

- a. Cliquez sur le bouton **Modifier**.

La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

- b. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

- c. Cliquez sur le bouton **OK**.

3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.



## Contrôle de la distribution des logiciels

► Pour ajouter un paquet de distribution de confiance, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Contrôle du lancement des applications**" à la page [396](#)).
2. Sous l'onglet **Contrôle de la distribution des logiciels**, cochez la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste**.

La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide des applications et des paquets d'installation repris dans la liste.

Si la case est cochée, l'application autorise automatiquement le lancement des fichiers exécutés à l'aide des distributions des paquets de confiance. La liste des applications et des paquets de distribution qui peuvent être lancés est modifiable.

Si la case est décochée, l'application ne tient pas compte des exclusions indiquées dans la liste.

Cette case est décochée par défaut.

**Vous pouvez cocher la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** si la case **Utiliser les règles pour les fichiers exécutables** sous l'onglet **Général** est cochée dans les paramètres de la tâche **Contrôle du lancement des applications**.**

3. Le cas échéant, décochez la case **Toujours autoriser la diffusion de logiciel via Windows Installer**.

La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide du sous-système Windows Installer.

Si la case est cochée, les fichiers installés via Windows Installer pourront toujours être lancés.

Si la case est décochée, le lancement sans condition des fichiers ne sera pas autorisé, même s'ils sont lancés via Windows Installer.

Cette case est cochée par défaut.

La case ne peut être modifiée si la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** n'est pas cochée.

**Il est conseillé de décocher la case **Toujours autoriser la diffusion de logiciel via Windows Installer** uniquement dans les cas extrêmes. La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.**

4. Le cas échéant, cochez la case **Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)**.

La case active ou désactive l'autorisation automatique de la diffusion du logiciel avec l'aide de la solution System Center Configuration Manager.

Si la case est cochée, Kaspersky Security for Windows Server autorise automatiquement le déploiement de Microsoft Windows à l'aide de System Center Configuration Manager.

L'application permet de distribuer une application uniquement à l'aide du service de transfert intelligent en arrière-plan (Background Intelligent Transfer Service).

L'application contrôle le lancement des objets qui portent les extensions suivantes :

- .exe
- .msi

Cette case est décochée par défaut.

L'application contrôle le cycle de distribution de logiciels sur le serveur, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de l'application sur le serveur.

5. Pour modifier la liste des paquets de distribution de confiance, cliquez sur le bouton **Modifier la liste de paquets** et sélectionnez une des méthodes suivantes dans la fenêtre qui s'ouvre :

- **Ajouter un paquet de distribution.**

a. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de lancement de l'application ou le paquet d'installation.

Les données du fichier sélectionné sont ajoutées automatiquement à la section **Critères de confiance**.

b. Cochez ou décochez la case **Autoriser le lancement de tous les fichiers extraits de ce paquet de distribution**.

c. Choisissez une de deux options proposées pour les critères de confiance qui vont déterminer si un fichier ou un paquet d'installation peut être considéré comme étant de confiance :

- **Utiliser un certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.

- **Utiliser le hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Ajouter plusieurs paquets selon le hash.**

Vous pouvez choisir un nombre illimité de fichiers de lancement et de paquets d'installation et les ajouter simultanément à la liste. Kaspersky Security for Windows Server tient compte du hash et autorise le lancement le système d'exploitation à lancer les fichiers indiqués.

- **Modifier le paquet sélectionné.**

Cette option permet de sélectionner un autre fichier de lancement ou un autre paquet d'installation. Elle permet également la modification des critères de confiance.

- **Importer la liste des paquets de distribution depuis un fichier.**

Vous pouvez importer la liste des paquets de distribution de confiance depuis un fichier de configuration. Pour être reconnu par Kaspersky Security for Windows Server, ce fichier doit répondre aux paramètres suivants :

- Le fichier possède l'extension TXT.
- contenir des informations présentées sur la forme d'une liste de lignes contenant chacune des données pour un des fichiers de confiance ;
- contenir une liste correspondant à un des deux formats suivants :
  - <nom du fichier>:<hash SHA256>.
  - <hash SHA256>\*<nom du fichier>.

Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des distributions des paquets de confiance.

6. Si vous voulez supprimer de la liste des éléments de confiance une application ou un paquet d'installation qui avait été ajouté antérieurement, cliquez sur le bouton **Supprimer les paquets d'installation**. Le lancement des fichiers extraits sera autorisé.

Pour interdire le lancement des fichiers extraits, désinstallez l'application du serveur protégé ou créez une règle d'interdiction dans les paramètres de la tâche Contrôle du lancement des applications.

7. Cliquez sur le bouton **OK**.

Les nouvelles valeurs des paramètres seront enregistrés.

## Configuration des règles du Contrôle du lancement des applications

Apprenez à créer, importer et exporter une liste de règles ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle du lancement des applications.

## Dans cette section

Ajout d'une règle de contrôle du lancement des applications .....	<a href="#">405</a>
Activation du mode Autoriser par défaut .....	<a href="#">408</a>
Création de règles d'autorisation au départ des événements de la tâche Contrôle du lancement des applications .....	<a href="#">408</a>
Exportation des règles du Contrôle du lancement des applications.....	<a href="#">409</a>
Importation des règles du Contrôle du lancement des applications depuis un fichier XML.....	<a href="#">409</a>
Suppression des règles du Contrôle du lancement des applications.....	<a href="#">410</a>

## Ajout d'une règle de contrôle du lancement des applications

► *Pour ajouter une règle de contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.  
La fenêtre **Paramètres de règle** s'ouvre.
4. Spécifiez les paramètres suivants :
  - a. Dans le champ **Nom**, saisissez le nom de la règle.
  - b. Dans la liste déroulante **Type**, sélectionnez le type de règle :
    - **Autorisé**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
    - **Interdit**, si vous souhaitez que la règle interdise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
  - c. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
    - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
    - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
  - d. Dans le champ **Utilisateur ou groupe d'utilisateurs**, indiquez les utilisateurs qui pourront ou non lancer des applications en fonction du type de règle. Pour ce faire, procédez comme suit :
    - i. Cliquez sur le bouton **Parcourir**.
    - ii. La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.
    - iii. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.
    - iv. Cliquez sur le bouton **OK**.
  - e. Réalisez les opérations suivantes si vous souhaitez extraire les valeurs pour les critères de déclenchement de la règle listés dans la section **Critères de déclenchement de la règle**, depuis un

fichier :

- i. Cliquez sur le bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**.

La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

- ii. Sélectionnez le fichier.
- iii. Cliquez sur le bouton **Ouvrir**.

Les valeurs des critères dans le fichier sont affichées dans les champs de la section **Critères de déclenchement de la règle**. Par défaut, c'est le premier critère de la liste dont les données figurent dans les propriétés du fichier qui est sélectionné.

- f. Dans la section **Critères de déclenchement de la règle**, sélectionnez une des options suivantes :
  - **Certificat numérique**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique :
    - Cochez la case **Utiliser l'objet**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'en-tête indiqué.
    - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle uniquement le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'empreinte indiquée.
  - **Hash SHA256**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers dont la somme de contrôle correspond à celle indiquée.
  - **Chemin du fichier**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.

Kaspersky Security for Windows Server ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

- g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :
  - i. Dans la section **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

La fenêtre **Exclusion de la règle** s'ouvre.
  - ii. Dans le champ **Nom**, saisissez le nom de l'exclusion.
  - iii. Indiquez les paramètres d'exclusions des fichiers des applications de la règle de contrôle du lancement des applications. Vous pouvez remplir les champs des paramètres depuis les propriétés du fichier en cliquant sur le bouton **Définir l'exclusion selon les propriétés du fichier**.
    - **Certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.
    - **Utiliser l'objet**

La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que

critère de déclenchement de la règle.

Si la case est cochée, l'objet du certificat numérique indiqué sera utilisé en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications uniquement pour l'éditeur repris dans l'en-tête.

Si la case est décochée, l'application n'utilise pas les en-têtes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, la règle créée contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quel en-tête.

L'en-tête du certificat numérique utilisé pour signer le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**

La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de déclenchement de la règle.

Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications signées par le certificat numérique doté de l'empreinte indiquée.

Si la case est décochée, l'application n'utilise pas l'empreinte de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, l'application contrôlera le lancement des applications signées à l'aide du certificat numérique doté n'importe quelle empreinte.

L'empreinte du certificat numérique utilisé pour signer le fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**, situé au-dessus de la section **Critères de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Chemin du fichier**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas

pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.

- iv. Cliquez sur le bouton **OK**.
- v. Si nécessaire, répétez les étapes (i) à (iv) pour ajouter des exclusions supplémentaires.

5. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

## Activation du mode Autoriser par défaut

La règle Autoriser par défaut autorise le lancement de toutes les applications si celui-ci n'est pas interdit par des règles ou par une conclusion de KSN qui les considère comme douteuses. Il est possible d'activer le mode Autoriser par défaut en ajoutant des règles d'autorisation spécifiques. Vous pouvez activer Autoriser par défaut uniquement pour les scripts ou pour tous les fichiers exécutables.

► *Pour ajouter une nouvelle règle Autoriser par défaut :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.  
La fenêtre **Paramètres de règle** s'ouvre.
4. Dans le champ **Nom**, saisissez le nom de la règle.
5. Dans la liste déroulante **Type**, sélectionnez le type de règle **Autorisé** :
6. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
  - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
  - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
7. Dans la section **Critères de déclenchement de la règle**, sélectionnez l'option **Chemin du fichier**.
8. Saisissez le masque suivant : ? : \
9. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique le mode Autoriser par défaut.

## Création de règles d'autorisation au départ des événements de la tâche Contrôle du lancement des applications

► *Pour créer un fichier de configuration qui contient les règles d'autorisation créées au départ des événements de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Lancez la tâche Contrôle du lancement des applications en mode **Statistiques uniquement** (cf. section "Sélection du mode la tâche Contrôle du lancement des applications" à la page [398](#)) pour consigner dans le journal d'exécution de la tâche les informations sur tous les lancements d'applications sur un ordinateur protégé.
2. A la fin de l'exécution de la tâche en mode **Statistiques uniquement**, ouvrez le journal d'exécution de la



tâche via le bouton **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du volet résultats du nœud **Contrôle du lancement des applications**.

3. Dans la fenêtre **Journaux**, appuyez sur **Créer des règles selon les événements**.

Kaspersky Security for Windows Server crée un fichier de configuration au format XML avec la liste des règles formées sur la base des événements de la tâche Contrôle du lancement des applications en mode **Statistiques uniquement**. Vous pouvez utiliser cette liste de règles (cf. section "Importation des règles du Contrôle du lancement des applications depuis un fichier XML" à la page [409](#)) dans la tâche Contrôle du lancement des applications.

Avant d'appliquer la liste des règles générées au départ des événements de tâche enregistrés, nous vous conseillons de réviser et de traiter manuellement la liste afin de confirmer que le lancement de fichiers critiques (par exemple, des fichiers systèmes) est autorisé par les règles définies.

Tous les événements de la tâche sont enregistrés dans le journal d'exécution de la tâche, quel que soit le mode de la tâche. Vous pouvez créer un fichier de configuration contenant une liste de règles basée sur le journal créé pour la tâche exécutée en mode **Actif**. Ce scénario est déconseillé, sauf pour les cas urgents, car une liste de règle définitive doit être créée avant de pouvoir exécuter la tâche en mode **Actif** afin de renforcer son efficacité.

## Exportation des règles du contrôle du lancement des applications

► *Pour exporter les règles du Contrôle du lancement des applications dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Cliquez sur le bouton **Exporter vers un fichier**.

La fenêtre standard de Microsoft Windows s'ouvre.

3. Dans la fenêtre qui s'ouvre, indiquez le fichier vers lequel vous souhaitez exporter les règles. Si ce fichier n'existe pas, il sera créé. Si un fichier portant ce nom existe déjà, son contenu sera écrasé après l'exportation des règles.

4. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la règle seront exportés dans le fichier indiqué.

## Importation des règles du Contrôle du lancement des applications depuis un fichier XML

► *Pour importer les règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Cliquez sur **Ajouter**.

3. Dans le menu contextuel du bouton, choisissez l'option **Importer les règles depuis un fichier au format XML**.

4. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez une des options du menu contextuel du bouton **Importer les règles depuis un fichier au format XML** :

- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.



- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

5. Dans la fenêtre **Ouvrir**, sélectionnez le fichier XML qui contient les règles du Contrôle du lancement des applications.
6. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du contrôle du lancement des applications**.

## Suppression des règles du contrôle du lancement des applications

► *Pour supprimer les règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer la sélection**.
4. Cliquez sur le bouton **Enregistrer**.

Les règles du Contrôle du lancement des applications sélectionnées seront supprimées.

## Configuration d'une tâche Génération des règles du Contrôle du lancement des applications

► *Pour configurer les paramètres de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications**" on page [397](#)) de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Configurez les paramètres suivants :
  - Sous l'onglet **Général** :
    - Indiquez le **Préfixe pour les noms des règles**.  
Il s'agit de la première partie du nom de la règle. La deuxième partie du nom de la règle est constituée à partir du nom de l'objet dont le lancement est autorisé.  
Par défaut, le nom du serveur sur lequel est installé Kaspersky Security for Windows Server est utilisé comme préfixe. Vous pouvez modifier le préfixe des noms des règles d'autorisation.
    - Configurez la zone d'application des règles d'autorisation (cf. Section "Restriction de la zone d'application de la tâche" à la page [411](#)).
  - Sous l'onglet **Action**, définissez les actions que Kaspersky Security for Windows Server doit réaliser :
    - Lors de la génération de règles d'autorisation (cf. section "Actions à réaliser lors de la génération

automatique de règles" à la page [412](#)).

- Une fois la tâche terminée (cf. section "Actions à réaliser à la fin de la génération automatique de règles" à la page [413](#)).
- Les onglets **Planification** et **Avancé** permettent de configurer les paramètres du lancement planifié de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)).
- L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page [160](#)).

3. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Informations sur la date et l'heure de modification des paramètres, et valeurs des paramètres de la tâche avant et après leur modification.

## Dans cette section

Restriction de la zone d'application de la tâche .....	<a href="#">411</a>
Actions à réaliser lors de la génération automatique de règles.....	<a href="#">412</a>
Actions à réaliser à la fin de la génération automatique de règles.....	<a href="#">413</a>

## Restriction de la zone d'application de la tâche

► *Pour limiter la zone d'application de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications**" on page [397](#)) de la tâche **Génération des règles du Contrôle du lancement des applications**.

2. Configurez les paramètres de la tâche suivants :

- **Créer des règles d'autorisation sur la base des applications en cours d'exécution.**

Cette case active ou désactive la création de règles du Contrôle du lancement des applications pour les applications déjà en cours d'exécution. Cette option est recommandée si une sélection d'applications de référence est en cours d'exécution sur le serveur et que vous souhaitez utiliser celle-ci pour générer les règles d'autorisation.

Si la case est cochée, les règles d'autorisation pour le contrôle du lancement des applications sont créées sur la base des applications exécutées.

Si la case est décochée, les applications en cours d'exécution ne sont pas prises en compte pour la génération des règles d'autorisation.

Cette case est cochée par défaut.

La case ne peut être décochée si aucun dossier n'est sélectionné dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**.

- **Créer des règles d'autorisation pour les applications des dossiers.**

Le tableau permet de sélectionner ou d'indiquer les dossiers pour la tâche et les types de

fichiers exécutables qui seront pris en compte lors de la génération des règles du Contrôle du lancement des applications. La tâche générera des règles d'autorisation pour les fichiers des types sélectionnés et situés dans les dossiers indiqués.

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Actions à réaliser lors de la génération automatique de règles

► *Pour configurer les actions que Kaspersky Security for Windows Server doit réaliser pendant l'exécution de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications**" on page [397](#)) de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Lors de la génération des règles d'autorisation** :

- **Utiliser un certificat numérique**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Nous recommandons cette option si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.

- **Utiliser l'objet et l'empreinte du certificat numérique**

La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique.

Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications. Kaspersky Security for Windows Server autorise désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique désignés.

L'utilisation de cette case limite fortement le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée.

Si la case est désélectionnée, un critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation.

La case est active si vous avez choisi l'option **Utiliser un certificat numérique**.

Cette case est cochée par défaut.

- **En cas d'absence de certificat, utiliser**

Il s'agit d'une liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le Contrôle du lancement des applications dans le cas où le fichier utiliser pour créer la règle ne dispose pas d'un certificat numérique.

- **hash SHA256.** La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
- **chemin du fichier.** Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.

- **Utiliser le hash SHA256**

Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.

Nous recommandons cette option pour les cas où les règles créées doivent garantir le plus haut niveau de sécurité possible : une somme de contrôle SHA256 peut être utilisée en tant qu'identifiant de fichier unique. L'utilisation de la somme de contrôle SHA256 en guise de critère de déclenchement de la règle limite la zone d'application des règles à un fichier.

Cette option est supprimée par défaut.

- **Créer des règles pour un utilisateur ou un groupe d'utilisateurs.**

Il s'agit d'un champ qui affiche un utilisateur ou un groupe d'utilisateurs. L'application contrôlera toutes les applications exécutées par l'utilisateur ou le groupe d'utilisateurs défini.

Par défaut, le groupe **Tous** est sélectionné.

4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

## Actions à réaliser à la fin de la génération automatique de règles

► *Pour configurer les actions que Kaspersky Security for Windows Server doit réaliser à la fin de la Génération des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "**Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications**" on page [397](#)) de la tâche **Génération des règles du Contrôle du lancement des applications**.

2. Ouvrez l'onglet **Options**.

3. Configurez les paramètres suivants dans la section **Une fois la tâche terminée** :

- **Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications.**

La case active ou désactive l'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications. La liste des règles du Contrôle du lancement des

applications est affichée via le lien **Règles du contrôle du lancement des applications** du panneau de détails du nœud Contrôle du lancement des applications.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les règles créées par la tâche Génération des règles du Contrôle du lancement des applications à la liste des règles du Contrôle du lancement des applications conformément au principe d'ajout défini.

Si la case est décochée, Kaspersky Security for Windows Server n'ajoute pas les règles d'autorisation créées à la liste de règles du Contrôle du lancement des applications. Les règles créées sont exportées uniquement dans un fichier.

Cette case est cochée par défaut.

- **Principe d'ajout.**

Il s'agit d'une liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications.

- **Ajouter aux règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes.** Les règles remplacent les règles existantes.
- **Fusionner avec les règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

Le mode **Fusionner avec les règles existantes** est sélectionné par défaut.

- **Exporter les règles d'autorisation vers un fichier.**

- **Ajouter des informations sur l'ordinateur dans le nom du fichier.**

La case active ou désactive l'ajout des informations relatives au serveur protégé au nom du fichier dans lequel sont exportées les règles d'autorisation du Contrôle des périphériques

Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur protégé ainsi que la date et l'heure de création du fichier.

Si la case est décochée, l'application n'ajoute pas les informations relatives au serveur protégé dans le nom du fichier d'exportation.

Cette case est cochée par défaut.

4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

# Contrôle des périphériques

Cette section contient les informations sur la tâche Contrôle des périphériques et les instructions de configuration de ses paramètres.

## Contenu du chapitre

A propos de la tâche Contrôle des périphériques .....	<a href="#">415</a>
A propos des règles du Contrôle des périphériques .....	<a href="#">416</a>
A propos de la formation de la liste des règles du Contrôle des périphériques .....	<a href="#">418</a>
A propos de la tâche Génération des règles du Contrôle des périphériques .....	<a href="#">420</a>
Scénarios de création de règles du Contrôle des périphériques .....	<a href="#">420</a>
Paramètres par défaut de la tâche Contrôle des périphériques .....	<a href="#">421</a>
Administration du Contrôle des périphériques via le plug-in d'administration .....	<a href="#">422</a>
Administration du Contrôle des périphériques via la Console de l'application .....	<a href="#">433</a>

## A propos de la tâche Contrôle des périphériques

Kaspersky Security for Windows Server contrôle l'enregistrement et l'utilisation des périphériques de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger le serveur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou d'autres types de périphérique externe connecté par USB. Un périphérique de stockage de masse est un périphérique externe qui peut être connecté à un serveur pour copier ou stocker des fichiers.

Kaspersky Security for Windows Server contrôle les connexions USB des périphériques externes suivants :

- Disques flash USB ;
- Lecteurs de CD ;
- Lecteurs de disquettes USB ;
- Périphériques mobiles MTP.USB.

Kaspersky Security for Windows Server vous informe des périphériques connectés via USB avec l'événement correspondant dans les journaux d'exécution des tâches et des événements. Les détails des événements incluent le type de périphérique et le chemin de connexion. Lors la tâche Contrôle des périphériques est lancée, Kaspersky Security for Windows Server analyse et énumère tous les périphériques connectés via USB. Vous pouvez configurer les notifications dans la section Configuration des notifications de Kaspersky Security Center.

La tâche Contrôle des périphériques surveille les tentatives de connexions USB de périphériques externes au serveur protégé et interdit leur utilisation en tant que stockages de masse s'il n'existe pas de règles d'autorisation pour ces périphériques. En raison du blocage, il est impossible de consulter le contenu du périphérique ou

d'exécuter des opérations sur les fichiers de ce périphérique (par exemple, lecture ou écriture des fichiers).

L'application attribuée à chaque périphérique de stockage de masse connecté un des états suivants :

- *De confiance*. Périphérique avec lequel l'échange de fichiers est autorisé. Lors de la génération d'une liste de règles, la valeur *Chemin d'accès à l'instance du périphérique* est incluse pour au moins une règle d'application.
- *Douteuse*. Périphérique avec lequel l'échange de données est interdit. Le chemin d'accès à l'instance d'un tel périphérique ne tombe pas sous le coup de la définition des règles d'autorisation.

Vous pouvez créer les règles d'autorisation pour les périphériques externes avec lesquels vous souhaitez autoriser l'échange de données à l'aide de la tâche Génération des règles du Contrôle des périphériques. Vous pouvez aussi élargir la zone d'application des règles d'autorisation déjà créées. Vous pouvez également créer des règles d'autorisation manuellement.

Kaspersky Security for Windows Server identifie les périphériques de stockage de masse enregistrés dans le système sur la base de la valeur du chemin d'accès à l'instance du périphérique. Le chemin d'accès à l'instance du périphérique est un élément unique pour chaque périphérique externe. La valeur du chemin d'accès à l'instance du périphérique est définie pour chaque périphérique externe dans ses propriétés Windows et est définie automatiquement par Kaspersky Security for Windows Server au moment de la création des règles.

La tâche Contrôle des périphériques peut être exécutée selon un des deux modes suivants :

- **Actif**. Kaspersky Security for Windows Server contrôle, à l'aide de règles, la connexion de disques flash et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe Interdire par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.

Si un périphérique externe que vous considérez douteux a été connecté à un serveur protégé avant le lancement de la tâche Contrôle des périphériques en mode **Actif**, ce périphérique n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement le périphérique douteux ou de redémarrer le serveur. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

- **Statistiques uniquement**. Kaspersky Security for Windows Server ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le serveur protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

Vous pouvez utiliser ce mode pour générer des règles sur la base des informations relatives à l'interdiction consignées pendant l'exécution de la tâche (cf. section "Composition de la liste des règles sur la base des événements de la tâche Contrôle des périphériques" à la page [437](#)).

## A propos des règles du Contrôle des périphériques

Les tâches sont créées individuellement pour chaque périphérique connecté au moment donné ou connecté auparavant au serveur protégé, si les données relatives à ce périphérique ont été mémorisées dans la base de registres système.

Pour créer des règles d'autorisation du contrôle des périphériques, vous pouvez effectuer une des opérations



suivantes :

- utiliser la tâche de génération des règles du Contrôle des périphériques (cf. section "A propos de la tâche Génération des règles pour le Contrôle des périphériques" à la page [420](#)) ;
- utiliser le mode Statistiques uniquement dans la tâche Contrôle des périphériques (cf. section "Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques" à la page [437](#)) ;
- utiliser les données système relatives aux périphériques connectés antérieurement (cf. section "Ajout d'une règle d'autorisation pour un ou plusieurs périphériques externes" à la page [438](#)) ;
- élargir le domaine d'application des règles existantes (cf. section "Extension de la zone d'application des règles de contrôle des périphériques" à la page [439](#)).

Le nombre maximum de règles du Contrôle des périphériques pris en charge par Kaspersky Security for Windows Server est égal à 3 072.

Les règles du Contrôle des périphériques sont décrites ci-après.

#### Type de règle

Les règles sont toujours des règles *Autorisé*. La tâche Contrôle des périphériques bloque par défaut les connexions de tous les disques flash et autres périphériques externes s'ils ne sont couverts par aucune règle d'autorisation.

#### Critères de déclenchement et zone d'application des règles

Les règles du Contrôle des périphériques identifient les disques flash et autres périphériques externes connectés à l'aide du *chemin d'accès à l'instance du périphérique*. Le chemin d'accès à l'instance du périphérique est un identifiant unique qui est attribué au périphérique par le système au moment de sa connexion et de l'enregistrement en tant que périphérique de stockage de masse ou de lecteur de CD/DVD (par exemple, IDE ou SCSI).

Kaspersky Security for Windows Server contrôle la connexion des lecteurs de CD/DVD, quel que soit le bus de connexion. Lors du montage de ces périphériques par connexion USB, le système d'exploitation enregistre deux valeurs du chemin d'accès à l'instance du périphérique : pour le périphérique de stockage de masse (Mass Storage) et pour le lecteur de CD/DVD (par exemple, IDE ou SCSI). La connexion adéquate de ces périphériques requiert l'existence de règles d'autorisation pour chaque valeur du chemin d'accès à l'instance du périphérique.

Kaspersky Security for Windows Server détermine automatiquement le chemin d'accès à l'instance du périphérique et scinde la valeur selon les composants suivants :

- Fabricant du périphérique (VID) ;
- Type de contrôleur du périphérique (PID) ;
- Numéro de série du périphérique.

Il est impossible de définir manuellement le chemin d'accès à l'instance du périphérique. Les critères de déclenchement de la règle définis dans les propriétés de la règle d'autorisation déterminent la zone d'application des règles. Par défaut, la zone d'application d'une règle qui vient d'être créée contient un périphérique dont les propriétés ont été exploitées par Kaspersky Security for Windows Server pour générer la règle. Vous pouvez configurer les valeurs dans la règle créée à l'aide d'un masque afin d'élargir la zone d'application des règles (cf. section "Extension de la zone d'application des règles de contrôle des périphériques" à la page [439](#)).



## Données du périphérique d'origine

Les propriétés du périphérique sur la base desquelles Kaspersky Security for Windows Server a créé la règle d'autorisation et qui s'affichent dans le gestionnaire de périphérique Windows pour chaque périphérique connecté.

Les données du périphérique contiennent les informations suivantes :

- **Chemin d'accès à l'instance du périphérique.** Sur la base de cette propriété, Kaspersky Security for Windows Server définit des critères de déclenchement de la règle et remplit les champs suivants : **Fabricant (VID), Type de contrôleur (PID), Numéro de série** dans la section **Zone d'application de la règle** de la fenêtre **Propriétés des règles**.
- **Nom convivial.** Nom attribué par le fabricant dans les propriétés du périphérique.

Kaspersky Security for Windows Server identifie automatiquement les données du périphérique d'origine lors de la création de la règle. Vous pourrez utiliser par la suite ces valeurs pour déterminer sur la base des données de quel périphérique la règle a été créée. Les données du périphérique d'origine ne peuvent être modifiées.

## Description

Vous pouvez ajouter des informations complémentaires pour chaque règle du Contrôle des périphériques créée dans le champ **Description**, par exemple, le nom du disque flash connecté ou le nom de son propriétaire. La description s'affiche dans la colonne correspondante du tableau de la fenêtre **Règles du Contrôle des périphériques**.

Les commentaires et les données du périphérique d'origine ne sont pas pris en compte lors du fonctionnement de la règle et servent uniquement à simplifier l'identification des appareils et des règles par l'utilisateur.

## A propos de la formation de la liste des règles du Contrôle des périphériques

Vous pouvez importer une liste de règles d'autorisation de contrôle des périphériques depuis des fichiers XML créés automatiquement lors de l'exécution de la tâche Contrôle des périphériques ou de la tâche Génération des règles du Contrôle des périphériques.

Par défaut Kaspersky Security for Windows Server interdit les connexions de n'importe quel disque flash et autre périphérique externe qui n'est pas soumis à l'action des règles du Contrôle des périphériques indiquées.

Tableau 58. Objectifs et scénarios de création de listes de règles de contrôle des périphériques

Scénarios de création de la liste des règles	Tâche à exécuter
Tâche Génération des règles du Contrôle des périphériques	<ul style="list-style-type: none"> <li>• Il faut créer des règles d'autorisation pour les périphériques de confiance déjà utilisés avant le premier lancement de la tâche Contrôle des périphériques.</li> <li>• Générez une liste des règles pour les périphériques de confiance dans le réseau de serveurs protégés.</li> </ul>
Génération de règles sur la base des données du système	Il faut ajouter des règles d'autorisation pour un ou plusieurs nouveaux périphériques connectés.

Tâche Contrôle des périphériques en mode **Statistiques uniquement**

Générez des règles d'autorisation pour un nombre important de nouveaux périphériques de confiance.

### Utilisation de la tâche Génération des règles du Contrôle des périphériques

Le fichier XML formé à la fin de la tâche Génération des règles du Contrôle des périphériques contient les règles d'autorisation pour les disques flash et autres périphériques externes dont les données de connexion sont mémorisées dans le système.

Au cours de l'exécution de la tâche, Kaspersky Security for Windows Server reçoit les données système relatives à tous les périphérique de stockage de masse qui ont été connectés à un moment donné ou qui sont connectés à un serveur protégé et génère une liste des règles d'autorisation sur la base des données système pour les périphériques détectés. A l'issue de la tâche, l'application crée un fichier XML dans le dossier accessible via le chemin d'accès indiqué dans les paramètres de la tâche. Vous pouvez configurer l'importation automatique des règles générées dans la liste de règles de la tâche Contrôle des périphériques.

Il est conseillé d'utiliser ce scénario pour composer la liste des règles d'autorisation avant le premier lancement de la tâche Contrôle des périphériques afin que les règles d'autorisation créées tiennent compte de tous les périphériques externes de confiance utilisés sur le serveur protégé.

### Utilisation des données système relatives à tous les périphériques connectés

Lors de l'exécution de la tâche, Kaspersky Security for Windows Server obtient les données système sur tous les périphériques externes connectés à un moment donné ou actuellement au serveur protégé et affiche les périphériques trouvés dans la liste de la fenêtre **Créer les règles sur la base des informations du système**.

Pour chaque périphérique trouvé, Kaspersky Security for Windows Server définit le fabricant (VID), le type de contrôleur (PID), le nom convivial, le numéro de série et le chemin d'accès à l'instance du périphérique. Vous pouvez créer des règles d'autorisation pour n'importe quel périphérique de stockage de masse dont les données ont été trouvées et ajouter directement les nouvelles règles à la liste des règles de contrôle des périphériques définies.

Il est conseillé d'utiliser ce scénario pour mettre à jour la liste des règles s'il faut autoriser l'utilisation d'un nombre limité de nouveaux périphériques de stockage de masse.

Kaspersky Security for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas générer des règles d'autorisation pour les périphériques mobiles MTP.

### Utilisation du rapport de la tâche Contrôle des périphériques en mode Statistiques uniquement

Le fichier XML obtenu à la fin de la tâche Contrôle des périphériques en mode **Statistiques uniquement** est créé sur la base du journal d'exécution de la tâche.

Au cours de l'exécution de la tâche, Kaspersky Security for Windows Server consigne les informations relatives à toutes les connexions de disques flash et autres périphérique de stockage de masse à un serveur protégé. Vous pouvez créer des règles d'autorisation en fonction des événements de la tâche et les exporter dans un fichier XML. Avant le lancement de la tâche en mode **Statistiques uniquement**, il est conseillé de configurer la période d'exécution de la tâche de telle sorte que toutes les connexions possibles de périphériques externes au serveur protégé puissent être réalisées dans le délai spécifié.

Ce scénario est recommandé pour actualiser une liste déjà générée de règles en cas de nécessité pour autoriser l'utilisation d'un grand nombre de nouveaux périphériques externes.

Si la composition de la liste des règles selon ce scénario se déroule sur une machine modèle, vous pouvez appliquer la liste créée des règles d'autorisation lors de la configuration de la stratégie du Contrôle des

périphériques dans Kaspersky Security Center. Ainsi, vous pourrez autoriser l'utilisation des périphériques externes connectés à la machine modèle sur tous les ordinateurs du réseau protégé.

## A propos de la tâche Génération des règles du Contrôle des périphériques

La tâche Génération des règles du Contrôle des périphériques permet de créer automatiquement une liste de règles d'autorisation pour les disques flash et autres périphériques de stockage de masse connectés sur la base des données du système relatives aux périphériques externes qui avaient été connectés auparavant à un serveur protégé.

Kaspersky Security for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas générer des règles d'autorisation pour les périphériques mobiles MTP.

À la fin de l'exécution de la tâche, Kaspersky Security for Windows Server crée un fichier de configuration au format XML qui contient la liste des règles d'autorisation pour tous les périphériques externes détectés ou ajoute directement les règles formées à la tâche Contrôle des périphériques en fonction des paramètres de la tâche Génération des règles du Contrôle des périphériques. L'application autorisera par la suite les périphériques pour lesquels des règles d'autorisation ont été générées automatiquement.

Les règles créées et ajoutées à la tâche figurent dans la fenêtre **Règles du Contrôle des périphériques**.

## Scénarios de création de règles du Contrôle des périphériques

Vous pouvez créer des règles (cf. section "Génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center" à la page [425](#)) sur la base des données Windows relatives aux périphériques de stockage de masse connectés par le passé ou actuellement selon trois scénarios :

- Avec l'aide de la tâche de groupe Génération des règles du Contrôle des périphériques. Utilisez ce scénario lors de la génération des règles pour prendre en compte tous les périphériques de stockage de masse connectés à un moment donné qui sont enregistrées par les systèmes sur tous les serveurs du réseau.
- Utilisation de l'option **Créer les règles sur la base des données du système**. Utilisez ce mode lors de la génération des règles pour prendre en compte tous les périphériques de stockage de masse enregistrés par le système du serveur doté de la Console d'administration de Kaspersky Security Center.
- A l'aide de l'option **Créer des règles sur la base des périphériques connectés** dans la fenêtre **Règles du Contrôle des périphériques** et des paramètres de la tâche Génération des règles du Contrôle des périphériques. Utilisez cette méthode si vous souhaitez que seules les données relatives aux périphériques connectés actuellement au serveur protégé soient prises en compte lors de la création des règles d'autorisation.

Kaspersky Security for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles de confiance connectés via MTP à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

## Paramètres par défaut de la tâche Contrôle des périphériques

La tâche Contrôle des périphériques possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 59. Paramètres par défaut de la tâche Contrôle des périphériques

Paramètre	Valeur par défaut	Description
<b>Mode de tâche</b>	<b>Statistiques uniquement</b>	La tâche consigne dans le journal d'exécution tous les événements d'interdiction et d'autorisation de connexion de périphériques externes conformément aux paramètres définis. Les périphériques externes ne sont pas vraiment bloqués. Vous pouvez choisir le mode <b>Actif</b> pour la protection d'un serveur afin d'appliquer l'interdiction de fait des périphériques externes.
<b>Autoriser l'utilisation de tous les périphériques de stockage de masse si la tâche Contrôle des périphériques n'est pas exécutée</b>	Pas appliqué	Kaspersky Security for Windows Server interdit l'utilisation des périphériques externes quel que soit l'état de l'exécution de la tâche Contrôle des périphériques. Cela garantit la protection maximale contre les menaces sur la sécurité informatique qui surgissent lors de l'échange de fichiers avec des périphériques externes. Vous pouvez configurer le paramètres de telle sorte que Kaspersky Security for Windows Server autorise l'utilisation de tous les périphériques externes si la tâche Contrôle des périphériques n'est pas exécutée.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Contrôle des périphériques n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server. Vous pouvez configurer la planification du lancement de la tâche.

Tableau 60. Paramètres par défaut de la tâche Génération des règles du Contrôle des périphériques

Paramètre	Valeur par défaut	Description
<b>Mode de tâche</b>	<b>Tenir compte des données du système sur tous les stockages de masse connectés à un moment donné</b>	

Paramètre	Valeur par défaut	Description
Actions une fois la tâche terminée	Les règles d'autorisation sont ajoutées à la liste des règles de contrôle des périphériques ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont effectués.	Vous pouvez ajouter des règles à des règles existantes sans fusion et sans suppression des doublons, ou remplacer les règles existantes par de nouvelles règles d'autorisation, ainsi que configurer les paramètres d'exportation des règles d'autorisation dans un fichier.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Génération des règles du Contrôle des périphériques n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

## Administration du Contrôle des périphériques via le plug-in d'administration

Cette section explique la navigation dans l'interface du plug-in d'administration et la gestion des connexions de n'importe quel périphérique de stockage de masse à tous les serveurs du réseau via la création de listes de règles à l'aide de Kaspersky Security Center pour les groupes de serveurs.

### Dans cette section

Navigation .....	<a href="#">422</a>
Configuration de la tâche Contrôle des périphériques .....	<a href="#">424</a>
Génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center .....	<a href="#">425</a>
Configuration de la tâche Génération des règles du Contrôle des périphériques.....	<a href="#">427</a>
Configuration de la tâche Contrôle des périphériques via Kaspersky Security Center .....	<a href="#">428</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres de la stratégie pour la tâche Contrôle des périphériques .....	<a href="#">423</a>
Accès à la liste des règles du Contrôle des périphériques.....	<a href="#">423</a>
Accès à l'assistant de la tâche Génération des règles du Contrôle des périphériques et aux propriétés .....	<a href="#">424</a>

## Accès aux paramètres de la stratégie pour la tâche Contrôle des périphériques

► *Pour accéder aux paramètres de la tâche Contrôle des périphériques via une stratégie de Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle des périphériques**.  
La fenêtre **Contrôle des périphériques** s'ouvre.
7. Configurez la stratégie en fonction des besoins.

## Accès à la liste des règles du Contrôle des périphériques

► *Pour accéder à la liste des règles du Contrôle des périphériques via Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle des périphériques**.  
La fenêtre **Contrôle des périphériques** s'ouvre.
7. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.  
La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
8. Configurez la stratégie en fonction des besoins.

## Accès à l'assistant de la tâche Génération des règles du Contrôle des périphériques et aux propriétés

► *Pour lancer la tâche Génération des règles du Contrôle des périphériques, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Cliquez sur le bouton **Créer une tâche**.

La fenêtre **Assistant de nouvelle tâche** s'ouvre.

5. Sélectionnez la tâche **Génération des règles du Contrôle des périphériques**.
6. Cliquez sur **Suivant**.

La fenêtre **Configuration** s'ouvre.

► *Pour configurer la tâche Génération des règles du Contrôle des périphériques existante, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

La fenêtre **Propriétés : Génération des règles du Contrôle des périphériques** s'ouvre.

Consultez la section Configuration de la tâche Génération des règles du Contrôle des périphériques pour en savoir plus sur la configuration de la tâche.

## Configuration de la tâche Contrôle des périphériques

► *Pour configurer les paramètres de la tâche Contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre **Contrôle des périphériques** (cf. section "Accès aux paramètres de la stratégie pour la tâche Contrôle des périphériques" à la page [423](#)).
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
  - Dans la section **Mode de tâche**, indiquez le mode de tâche :
    - **Actif**.

Kaspersky Security for Windows Server contrôle, à l'aide de règles, la connexion de disques flash et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe Interdire par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.



Si un périphérique externe que vous considérez douteux a été connecté à un serveur protégé avant le lancement de la tâche Contrôle des périphériques en mode Actif, ce périphérique n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement le périphérique douteux ou de redémarrer l'ordinateur. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

- **Statistiques uniquement.**

Kaspersky Security for Windows Server ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le serveur protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

- Décochez ou cochez la case **Autoriser l'utilisation de tous les périphériques de stockage de masse si la tâche Contrôle des périphériques n'est pas exécutée.**

La case autorise ou interdit l'utilisation des périphériques de stockage de masse quand la tâche Contrôle des périphériques est arrêtée.

Si la case est cochée et que la tâche Contrôle des périphériques n'est pas exécutée, Kaspersky Security for Windows Server autorise l'utilisation de n'importe quel périphérique stockage de masse sur un serveur protégé.

Si la case est décochée, l'application interdit l'utilisation des périphériques de stockage de masse douteux sur un serveur protégé quand la tâche Contrôle des périphériques n'est pas exécutée ou que le service Kaspersky Security est désactivé. Il est conseillé d'utiliser cette version pour garantir la protection maximale contre les menaces sur la sécurité informatique qui surgissent lors de l'échange de fichiers avec des périphériques externes.

Cette case est décochée par défaut.

3. Cliquez sur le bouton **Liste des règles** de la liste pour modifier la liste des règles du Contrôle des périphériques (cf. section "Configuration de la tâche Contrôle des périphériques via Kaspersky Security Center" à la page [428](#)).
4. Le cas échéant, configurez les paramètres de la planification du lancement de la tâche sous l'onglet **Administration des tâches**.
5. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

## Génération des règles du Contrôle des périphériques pour l'ensemble des ordinateurs via Kaspersky Security Center

Vous pouvez créer des listes de règles de contrôle des périphériques à l'aide de tâches de Kaspersky Security Center directement pour tous les serveurs et groupes de serveurs du réseau de l'organisation.

Vous pouvez créer des listes de règles du Contrôle des périphériques dans Kaspersky Security Center de la manière suivante :



- Avec l'aide de la tâche de groupe Génération des règles du Contrôle des périphériques.

D'après ce scénario, la tâche de groupe compose les listes des règles sur la base des données du système de chaque ordinateur relatives à tous les périphériques de stockage de masse jamais connectés aux serveurs protégés. La tâche tient également compte de tous les périphériques de stockage de masse connectés au moment de l'exécution de la tâche de groupe. À la fin de l'exécution de la tâche de groupe, Kaspersky Security for Windows Server compose les listes des règles d'autorisation pour tous les périphériques de stockage de masse du réseau enregistrés et enregistre ces listes dans un fichier XML dans le dossier indiqué. Vous pouvez ensuite importer manuellement les listes de règles composées dans les propriétés de la stratégie Contrôle des périphériques. A la différence d'une tâche sur l'ordinateur local, la stratégie n'accepte pas la configuration de l'ajout automatique des règles créées dans la liste des règles de contrôle des périphériques à la fin de la tâche de groupe Génération des règles du Contrôle des périphériques.

Il est recommandé d'utiliser ce scénario pour composer une liste de règles d'autorisation avant le premier lancement de la tâche Contrôle des périphériques en mode d'application active des règles.

Avant d'appliquer la stratégie de Contrôle des périphériques, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

- Sur la base du rapport généré dans Kaspersky Security Center et relatif aux événements survenus pendant le fonctionnement de la tâche Contrôle des périphériques en mode **Statistiques uniquement**.

D'après ce scénario, Kaspersky Security for Windows Server ne limite pas les connexions des périphériques de stockage de masse, mais consigne toutes les connexions des périphériques et l'enregistrement des périphériques de stockage de masse sur tous les serveurs de réseau pendant la période de fonctionnement de la tâche de contrôle des périphériques en mode **Statistiques uniquement**. Les informations enregistrées sont disponibles sous l'onglet **Événements** de l'espace de travail du nœud **Serveur d'administration** dans Kaspersky Security Center. Kaspersky Security Center établit ensuite, sur la base du journal d'exécution de la tâche, une liste unique des événements de blocage et de connexion des périphériques de stockage de masse.

Vous devez configurer la période de l'exécution de la tâche de telle sorte que toutes les connexions de périphériques de stockage de masse puissent avoir lieu au cours de la période indiquée. Par la suite, lors de l'ajout de règles à la tâche de contrôle des périphériques, vous pouvez importer les données relatives aux connexions de périphériques depuis le fichier de rapport sur les événements de Kaspersky Security Center enregistré au format TXT et créer, sur la base de ces données, des règles d'autorisation pour le contrôle de ces périphériques. Les règles d'autorisations sont créées à l'importation du journal créé sur la base des événements de n'importe quel type.

Il est conseillé d'utiliser ce scénario s'il faut ajouter des règles d'autorisation pour un nombre important de nouveaux périphériques de stockage de masse et pour créer des règles d'autorisation pour les périphériques mobiles de confiance connectés via le protocole MTP.

- Sur la base des données système relatives aux périphériques de stockage de masse connectés (à l'aide de l'option **Créer les règles sur la base des données du système** dans les paramètres de la tâche Contrôle des périphériques).

Dans le cadre ce scénario, Kaspersky Security for Windows Server compose les règles d'autorisation pour les périphériques de stockage de masse connectés auparavant ou connectés actuellement à l'ordinateur doté de Kaspersky Security Center.

Il est recommandé d'utiliser ce scénario quand il faut générer des règles pour un nombre réduit de

nouveaux périphériques de stockage de masse dont vous souhaitez autoriser l'utilisation sur tous les serveurs du réseau.

- Sur la base des données relatives aux périphériques connectés actuellement (à l'aide de l'option **Créer des règles sur la base des périphériques connectés**).

Dans le cadre de ce scénario, Kaspersky Security for Windows Server crée des règles d'autorisation uniquement pour les périphériques connectés actuellement. Vous pouvez sélectionner un ou plusieurs périphériques pour lesquels vous souhaitez confirmer des règles d'autorisation.

Kaspersky Security for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles de confiance connectés via MTP à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

## Configuration de la tâche Génération des règles du Contrôle des périphériques

► Pour configurer les paramètres de la tâche Génération des règles du Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle des périphériques** (cf. section "**Accès à l'assistant de la tâche Génération des règles du Contrôle des périphériques et aux propriétés**" à la page [424](#)).
2. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

3. La section **Configuration** permet de configurer les paramètres suivants :
  - sélectionnez le mode de fonctionnement : tenir compte des données système relatives à tous les périphériques de stockage de masse jamais connectés ou tenir compte uniquement des périphériques de stockage de masse connecté actuellement.
  - Configurez les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Security for Windows Server crée à la fin des tâches.
4. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
5. Dans la section **Compte utilisateur**, désignez le compte avec les privilèges duquel vous souhaitez exécuter la tâche.
6. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

7. Dans la fenêtre **Propriétés : <nom de la tâche>**, cliquez sur **OK**.

Les paramètres des tâches de groupe définis seront enregistrés.

## Configuration de la tâche **Contrôle des périphériques** via Kaspersky Security Center

Apprenez à créer une liste de règles sur la base de différents critères ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche **Contrôle des périphériques**.

### Dans cette section

Création de règles d'autorisation sur la base des données du système dans une stratégie de Kaspersky Security Center .....	<a href="#">428</a>
Création de règles pour les périphériques connectés .....	<a href="#">429</a>
Importation des règles depuis un rapport de Kaspersky Security Center sur les périphériques bloqués .....	<a href="#">429</a>
Création de règles à l'aide de la tâche Génération des règles du Contrôle des périphériques .....	<a href="#">431</a>
Ajout des règles créées à la liste des règles du Contrôle des périphériques .....	<a href="#">433</a>

### Création de règles d'autorisation sur la base des données du système dans une stratégie de Kaspersky Security Center

- *Pour définir les règles d'autorisation à l'aide de l'option **Créer les règles sur la base des données du système**, dans les paramètres de la tâche **Contrôle des périphériques**, procédez comme suit :*

1. Le cas échéant, connectez à l'ordinateur doté de la console d'administration de Kaspersky Security Center un nouveau périphérique de stockage de masse dont vous souhaitez autoriser l'utilisation.
2. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Accès à la liste des règles du Contrôle des périphériques" à la page [423](#)).
3. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.
4. Sélectionnez le principe d'ajout des règles d'autorisation à la liste des règles de contrôle des périphériques déjà créées :
  - Dans la liste de périphériques de la fenêtre **Créer les règles sur la base des informations du système**, sélectionnez un périphérique.
  - Cliquez sur **Ajouter des règles pour les périphériques sélectionnés**.
5. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

La liste des règles dans la tâche **Contrôle des périphériques** sera enrichie de nouvelles règles formées sur la base des données du système de l'ordinateur sur lequel la Console d'administration de Kaspersky Security

Center est installée.

## Création de règles pour les périphériques connectés

► *Pour définir les règles d'autorisation à l'aide de l'option **Créer des règles sur la base des périphériques connectés**, dans la tâche **Contrôle des périphériques**, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Accès à la liste des règles du Contrôle des périphériques" à la page [423](#)).
2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer des règles sur la base des périphériques connectés**.

La fenêtre **Créer les règles sur la base des informations du système** s'ouvre.

3. Dans la liste des périphériques détectés qui sont connectés au serveur protégé, choisissez les périphériques pour lesquels vous voulez créer des règles d'autorisation.
4. Cliquez sur le bouton **Ajouter des règles pour les périphériques sélectionnés**.
5. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

La liste des règles dans la tâche **Contrôle des périphériques** sera enrichie de nouvelles règles formées sur la base des données du système de l'ordinateur sur lequel la Console d'administration de Kaspersky Security Center est installée.

## Importation des règles depuis un rapport de Kaspersky Security Center sur les périphériques bloqués

Vous pouvez importer les données relatives aux connexions des périphériques bloqués depuis le rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche **Contrôle des périphériques** en mode **Statistiques uniquement** (cf. section "Configuration de la tâche **Contrôle des périphériques**" à la page [424](#)) et appliquer ces données à la composition d'une liste de règles d'autorisation du **Contrôle des périphériques** dans la stratégie configurée.

Lors de la création du rapport sur les événements survenus pendant l'exécution de la tâche de contrôle des périphériques, vous pouvez surveiller la connexion des périphériques qu'il faudra bloquer.

► *Pour créer des règles d'autorisation de connexion des périphériques pour un groupe de serveurs sur la base d'un rapport de Kaspersky Security Center relatif aux périphériques bloqués, procédez comme suit :*

1. Dans la section **Notifications sur les événements** des propriétés de la stratégie, assurez-vous que :
  - S'agissant du niveau d'importance **Événements critiques**, la durée de conservation du journal d'exécution de la tâche pour l'événement *Stockage de masse restreint* dépasse la période de fonctionnement prévue du mode **Statistiques uniquement** (la valeur par défaut est de 30 jours).
  - S'agissant du niveau d'importance **Avertissement**, la durée de conservation du journal d'exécution de la tâche pour l'événement *Statistiques uniquement : périphérique de stockage de masse inconnu détecté* dépasse la période de fonctionnement prévue du mode **Statistiques uniquement** (la valeur par défaut est de 30 jours).

A l'échéance de la période de conservation des événements, les informations relatives aux événements enregistrés seront supprimées et ne figureront pas dans le fichier du rapport. Avant de lancer la tâche Contrôle des périphériques en mode **Statistiques uniquement**, assurez-vous que la durée d'exécution de la tâche n'est pas supérieure à la durée de conservation établie pour les événements indiqués.

2. Lancez la tâche Contrôle des périphériques en mode **Statistiques uniquement**. Dans l'espace de travail du nœud **Serveur d'administration** de Kaspersky Security Center, sélectionnez l'onglet **Événements**. Cliquez sur le bouton **Créer une sélection** pour créer une sélection d'événements sur la base du critère *Détection d'un périphérique de stockage de masse douteux* pour voir les périphériques dont les connexions vont être limitées par la tâche Contrôle des périphériques. Dans le volet des détails de la sélection, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites dans un fichier au format TXT.

Avant d'importer et d'appliquer un rapport créé dans une stratégie, assurez-vous qu'il contient les données relatives uniquement aux périphériques dont vous souhaitez autoriser la connexion.

3. Importez les données sur les tentatives bloquées de connexion des périphériques dans la tâche du Contrôle des périphériques :
  - a. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Accès à la liste des règles du Contrôle des périphériques" à la page [423](#)).
  - b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel, sélectionnez l'option **Importer les données relatives aux périphériques bloqués depuis le rapport de Kaspersky Security Center**.
  - c. Sélectionnez le principe d'ajout des règles depuis la liste créée sur la base du rapport de Kaspersky Security Center à la liste des règles du Contrôle des périphériques existantes :
    - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
    - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
    - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.
  - d. Dans la fenêtre Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les périphériques bloqués ont été exportés.
  - e. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.
4. Cliquez sur **OK** dans la fenêtre **Contrôle des périphériques**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les périphériques bloqués seront ajoutées à la liste des règles de la stratégie de contrôle des périphériques.

## Création de règles à l'aide de la tâche Génération des règles du Contrôle des périphériques

► Pour définir les règles d'autorisation du contrôle des périphériques pour un groupe de serveurs à l'aide de la tâche Génération des règles du Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Configuration** dans l'**Assistant Nouvelle tâche** (cf. section "**Accès à l'assistant de la tâche Génération des règles du Contrôle des périphériques et aux propriétés**" à la page [424](#)).
2. Configurez les éléments suivants :

- Dans la section **Mode** :
  - **Tenir compte des données du système sur tous les stockages de masse connectés à un moment donné.**
  - **Tenir compte des données sur les stockages de masse connectés actuellement.**
- Dans la section **Une fois la tâche terminée** :

- **Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques.**

La case active ou désactive l'ajout des règles d'autorisation créées à la liste des règles du Contrôle des périphériques. La liste des règles du Contrôle des périphériques est affichée via le lien **Règles du Contrôle des périphériques** du volet des détails du nœud **Contrôle des périphériques**.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les règles créées au cours de l'exécution de la tâche Génération des règles du Contrôle des périphériques à la liste de règles du Contrôle des périphériques conformément au principe d'ajout défini.

Si la case est décochée, Kaspersky Security for Windows Server n'ajoute pas les règles d'autorisation créées à la liste de règles du Contrôle des périphériques. Les règles créées sont exportées uniquement dans un fichier.

Cette case est cochée par défaut.

La case ne peut être décochée si la case **Exporter les règles d'autorisation vers un fichier** n'est pas cochée.

- **Principe d'ajout.**

Il s'agit d'une liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications.

- **Ajouter aux règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes.** Les règles remplacent les règles existantes.
- **Fusionner avec les règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

Le mode **Fusionner avec les règles existantes** est sélectionné par défaut.

- **Exporter les règles d'autorisation vers un fichier.**

La case active ou désactive l'exportation des règles d'autorisation pour le contrôle des périphériques vers un fichier.

Si la case est cochée, Kaspersky Security for Windows Server exporte les règles d'autorisation vers le fichier indiqué dans le champ ci-dessous, une fois la tâche Génération des règles du Contrôle des périphériques terminée.

Quand cette case est décochée, l'application n'exporte pas les règles d'autorisation générées dans un fichier à la fin de la tâche Génération des règles du Contrôle des périphériques. Elle se contente de les ajouter à la liste des règles du Contrôle des périphériques.

Cette case est décochée par défaut.

La case ne peut pas être cochée si la case **Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques** n'est pas cochée.

- **Ajouter des informations sur l'ordinateur dans le nom du fichier.**

La case active ou désactive l'ajout des informations relatives au serveur protégé au nom du fichier dans lequel sont exportées les règles d'autorisation du Contrôle des périphériques

Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur protégé ainsi que la date et l'heure de création du fichier.

Si la case est décochée, l'application n'ajoute pas les informations relatives au serveur protégé dans le nom du fichier d'exportation.

Cette case est cochée par défaut.

3. Cliquez sur **Suivant**.
4. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.
5. Cliquez sur **Suivant**.
6. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.
7. Cliquez sur **Suivant**.
8. Définissez un nom de tâche.
9. Cliquez sur **Suivant**.

Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants :  
" \* < > & \ : |

La fenêtre **Fin de la création de la tâche** s'ouvre.

10. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.
11. Cliquez sur **Terminer** pour terminer la création de la tâche.
12. Sous l'onglet **Tâches** de l'espace de travail du groupe de serveurs configurés, sélectionnez la tâche Génération des règles du Contrôle des périphériques dans la liste des tâches de groupe.
13. Cliquez sur le bouton **Démarrer** pour démarrer la tâche.

A l'issue de la tâche, les listes de règles d'autorisation générées automatiquement seront enregistrées dans le dossier partagé dans des fichiers XML.



Avant d'appliquer la stratégie de Contrôle des périphériques, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les serveurs protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est conseillé de lancer la tâche de génération automatique de règles du contrôle du serveur sur un groupe d'ordinateurs d'essai ou sur une machine modèle.

## Ajout des règles créées à la liste des règles du Contrôle des périphériques

► Pour ajouter les listes de règles d'autorisation créées à la tâche Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Accès à la liste des règles du Contrôle des périphériques" à la page [423](#)).
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Importer les règles depuis un fichier au format XML**.
4. Sélectionnez le principe d'ajout des règles d'autorisation générées automatiquement à la liste des règles de contrôle des périphériques déjà créées :
  - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
  - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
  - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.
5. Dans la fenêtre Windows standard qui s'ouvre, choisissez les fichiers au format XML créés à l'issue de la tâche de groupe Génération des règles du Contrôle des périphériques.
6. Cliquez sur **Ouvrir**.

Toutes les règles générées depuis le fichier XML sont ajoutées à la liste conformément au principe sélectionné.
7. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.
8. Si vous voulez appliquer les règles créées pour le Contrôle des périphériques, sélectionnez le mode de tâche **Actif** dans les paramètres de la stratégie **Contrôle des périphériques**.

Les règles d'autorisation générées automatiquement sur la base des données du système sur chaque serveur distinct sont appliquées à tous les serveurs du réseau soumis à la stratégie configurée. Pour ces serveurs, l'application autorise la connexion des périphériques pour lesquels des règles d'autorisation ont été créées.

## Administration du Contrôle des périphériques via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un serveur local.



## Dans cette section

Navigation .....	<a href="#">434</a>
Configuration des paramètres de la tâche Contrôle des périphériques .....	<a href="#">435</a>
Configuration des règles du Contrôle des périphériques .....	<a href="#">436</a>
Configuration de la tâche Génération des règles du Contrôle des périphériques.....	<a href="#">440</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres de la tâche Contrôle des périphériques .....	<a href="#">434</a>
Ouverture de la fenêtre des règles du Contrôle des périphériques.....	<a href="#">434</a>
Accès aux paramètres de la tâche Génération des règles du Contrôle des périphériques .....	<a href="#">435</a>

## Accès aux paramètres de la tâche Contrôle des périphériques

► *Pour accéder aux paramètres de la tâche Contrôle des périphériques via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Contrôle des périphériques**.
3. Dans le volet des détails du nœud enfant **Contrôle des périphériques**, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez la tâche en fonction des besoins.

## Ouverture de la fenêtre des règles du Contrôle des périphériques

► *Pour ouvrir la liste des règles du Contrôle des périphériques via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Contrôle des périphériques**.
3. Dans le volet des détails du nœud **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.  
La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
4. Configurez la liste des règles en fonction des besoins.

## Accès aux paramètres de la tâche Génération des règles du Contrôle des périphériques

► Pour configurer la tâche Génération des règles du Contrôle des périphériques, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Choisissez le nœud enfant **Génération des règles du Contrôle des périphériques**.
3. Dans le volet des détails du nœud enfant **Génération des règles du Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

4. Configurez la tâche en fonction des besoins.

## Configuration des paramètres de la tâche Contrôle des périphériques

► Pour configurer les paramètres de la tâche Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** (cf. section "Accès aux paramètres de la tâche Contrôle des périphériques" à la page [434](#)).
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
  - Dans la section **Mode de tâche**, indiquez le mode de tâche :
    - **Actif**.

Kaspersky Security for Windows Server contrôle, à l'aide de règles, la connexion de disques flash et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe Interdire par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.

Si un périphérique externe que vous considérez douteux a été connecté à un serveur protégé avant le lancement de la tâche Contrôle des périphériques en mode Actif, ce périphérique n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement le périphérique douteux ou de redémarrer l'ordinateur. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

- **Statistiques uniquement**.

Kaspersky Security for Windows Server ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le serveur protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

- Décochez ou cochez la case **Autoriser l'utilisation de tous les périphériques de stockage de masse si la tâche Contrôle des périphériques n'est pas exécutée**.

La case autorise ou interdit l'utilisation des périphériques de stockage de masse quand la

tâche Contrôle des périphériques est arrêtée.

Si la case est cochée et que la tâche Contrôle des périphériques n'est pas exécutée, Kaspersky Security for Windows Server autorise l'utilisation de n'importe quel périphérique stockage de masse sur un serveur protégé.

Si la case est décochée, l'application interdit l'utilisation des périphériques de stockage de masse douteux sur un serveur protégé quand la tâche Contrôle des périphériques n'est pas exécutée ou que le service Kaspersky Security est désactivé. Il est conseillé d'utiliser cette version pour garantir la protection maximale contre les menaces sur la sécurité informatique qui surgissent lors de l'échange de fichiers avec des périphériques externes.

Cette case est décochée par défaut.

3. Les onglets **Planification** et **Avancé** permettent de configurer, le cas échéant, les paramètres de lancement planifié de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)).
4. Pour modifier la liste des règles du Contrôle des périphériques (cf. section "A propos de la formation de la liste des règles du Contrôle des périphériques" à la page [418](#)), cliquez sur le lien **Règles du Contrôle des périphériques** dans la partie inférieure du volet des détails du nœud **Contrôle des périphériques**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

## Configuration des règles du Contrôle des périphériques

Apprenez à créer, importer et exporter une liste de règles ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle des périphériques.

### Dans cette section

Importation des règles du Contrôle des périphériques depuis un fichier XML.....	<a href="#">436</a>
Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques.....	<a href="#">437</a>
Ajout d'une règle d'autorisation pour un ou plusieurs périphériques externes.....	<a href="#">438</a>
Suppression des règles du Contrôle des périphériques.....	<a href="#">438</a>
Exportation des règles du Contrôle des périphériques.....	<a href="#">439</a>
Activation et désactivation des règles du Contrôle des périphériques.....	<a href="#">439</a>
Extension de la zone d'application des règles du Contrôle des périphériques.....	<a href="#">439</a>

### Importation des règles du Contrôle des périphériques depuis un fichier XML

► *Pour importer des règles de contrôle de contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "**Ouverture de la fenêtre des règles du Contrôle des périphériques**" à la page [434](#)).
2. Cliquez sur **Ajouter**.

3. Dans le menu contextuel du bouton, choisissez l'option **Importer les règles depuis un fichier au format XML**.
4. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez une des options du menu contextuel du bouton **Importer les règles depuis un fichier au format XML** :
  - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
  - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
  - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

5. Dans la fenêtre **Ouvrir**, sélectionnez le fichier XML qui contient les paramètres des règles du Contrôle des périphériques.
6. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du Contrôle des périphériques**.

## Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques

- *Pour créer un fichier de configuration contenant la liste des règles du Contrôle des périphériques créées sur la base des événements de la tâche Contrôle des périphériques, procédez comme suit :*
1. Lancez la tâche Contrôle des périphériques en mode **Statistiques uniquement** (cf. section "**Configuration des paramètres de la tâche Contrôle des périphériques**" à la page [435](#)) pour consigner tous les événements de connexion de disques flash ou d'autres périphériques externes à un serveur protégé.
  2. A la fin de la tâche en mode **Statistiques uniquement**, ouvrez le journal d'exécution de la tâche via le bouton **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du panneau des détails du nœud **Contrôle des périphériques**.
  3. Dans la fenêtre **Journaux**, cliquez sur le bouton **Créer des règles selon les événements**.

Kaspersky Security for Windows Server crée un fichier de configuration au format XML qui contient une liste des règles composées selon les événements de la tâche Contrôle des périphériques en mode **Statistiques uniquement**. Vous pouvez appliquer cette liste dans la tâche Contrôle des périphériques (cf. section "Importation des règles de contrôle des périphériques depuis un fichier XML" à la page [436](#)).

Avant d'appliquer la liste des règles formée selon les événements de la tâche, il est recommandé de l'examiner, et puis de traiter manuellement la liste des règles pour confirmer que les règles définies interdisent la connexion des périphériques douteux.

Lors de la conversion du fichier XML contenant les événements d'exécution de la tâche en liste de règles de contrôle des périphériques, l'application crée les règles d'autorisation pour tous les événements enregistrés, y compris pour les événements d'interdiction de périphériques.

Tous les événements de la tâche sont enregistrés dans le journal d'exécution de la tâche dans chacun des deux modes. Vous pouvez créer le fichier de configuration contenant une liste des règles sur la base des événements de la tâche en mode **Actif**. Ce scénario n'est pas recommandé, sauf en cas d'urgence, car l'exécution efficace de la tâche requiert la composition d'une liste de règles finale avant le lancement de la tâche en mode actif.

## Ajout d'une règle d'autorisation pour un ou plusieurs périphériques externes

La tâche du contrôle des périphériques ne prévoit pas la fonction d'ajout d'une règle manuellement. Cependant, si vous devez ajouter des règles d'autorisation pour un ou plusieurs nouveaux périphériques externes, vous pouvez utiliser l'option **Créer les règles sur la base des données du système**. Lors de l'utilisation de ce scénario, l'application utilise les données de Windows relatives à tous les périphériques externes connectés et autorise les périphériques externes connectés en ce moment de remplir une liste des règles d'autorisation.

Kaspersky Security for Windows Server n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas générer des règles d'autorisation pour les périphériques mobiles MTP.

► *Pour ajouter une règle d'autorisation pour un ou plusieurs périphériques externes utilisés en ce moment, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Ouverture de la fenêtre des règles du Contrôle des périphériques" à la page [434](#)).
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.
4. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste des périphériques détectés le ou les périphériques dont vous souhaitez autoriser l'utilisation sur un serveur protégé.
5. Cliquez sur le bouton **Ajouter des règles pour les périphériques sélectionnés**.

Les nouvelles règles seront ajoutées à la liste des règles de contrôle des périphériques.

## Suppression des règles du Contrôle des périphériques

► *Pour supprimer des règles du Contrôle des périphériques :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "Ouverture de la fenêtre des règles du Contrôle des périphériques" à la page [434](#)).
2. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer la sélection**.
4. Cliquez sur le bouton **Enregistrer**.

Les règles de contrôle des périphériques sélectionnées seront supprimées.

## Exportation des règles du Contrôle des périphériques

► *Pour exporter les règles du Contrôle des périphériques dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "**Ouverture de la fenêtre des règles du Contrôle des périphériques**" à la page [434](#)).
2. Cliquez sur le bouton **Exporter vers un fichier**.

La fenêtre standard de Microsoft Windows s'ouvre.

3. Dans la fenêtre qui s'ouvre, indiquez le fichier vers lequel vous souhaitez exporter les règles. Si ce fichier n'existe pas, il sera créé. Si un fichier portant ce nom existe déjà, son contenu sera écrasé après l'exportation des règles.
4. Cliquez sur le bouton **Enregistrer**.

Les règles et leurs paramètres seront exportés dans le fichier indiqué.

## Activation et désactivation des règles du Contrôle des périphériques

Vous pouvez activer et désactiver l'application des règles d'autorisation créées pour le contrôle des périphériques sans les supprimer.

► *Pour activer ou désactiver une règle créée du Contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "**Ouverture de la fenêtre des règles du Contrôle des périphériques**" à la page [434](#)).
2. Dans la liste des règles définies, ouvrez la fenêtre **Propriétés des règles** d'un double clic sur la règle dont vous souhaitez configurer les propriétés.
3. Dans la fenêtre qui s'ouvre, décochez ou cochez la case **Appliquer la règle**.

La case active ou désactiver l'application de la règle du Contrôle des périphériques.

Si la case est cochée dans les paramètres de la règle, la règle est active. La connexion des périphériques externes couverts par la zone d'application de cette règle sera autorisée.

Si la case est décochée dans les paramètres de la règle, cette règle est inactive. La connexion des périphériques externes couverts par la zone d'application de cette règle sera interdite.

La case est cochée par défaut dans les paramètres de chaque règle créée.

4. Cliquez sur le bouton **OK**.

L'état de l'application de la règle est enregistré et s'affiche pour la règle indiquée.

## Extension de la zone d'application des règles du Contrôle des périphériques

Chaque règle du contrôle des périphériques créée automatiquement autorise la connexion d'un seul périphérique externe. Vous pouvez élargir manuellement la zone d'application des règles en introduisant un masque de chemin d'accès à l'instance du périphérique dans les paramètres de n'importe quelle règle de contrôle des périphériques

créée.

L'application du masque du chemin d'accès à l'instance du périphérique diminue la quantité de règles d'autorisation du contrôle des périphériques et simplifie le processus de leur traitement manuel. Cependant, l'extension de la zone d'application des règles peut réduire l'efficacité du contrôle des périphériques de stockage de masse.

► Pour appliquer le masque de chemin d'accès à l'instance du périphérique dans les propriétés d'une règle du Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques** (cf. section "**Ouverture de la fenêtre des règles du Contrôle des périphériques**" à la page [434](#)).
2. Dans la fenêtre qui s'ouvre, choisissez une règle afin d'utiliser ses propriétés pour l'application d'un masque.
3. Ouvrez la fenêtre **Propriétés des règles** d'un double clic sur la règle du Contrôle des périphériques choisie.
4. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
  - Cochez la case **Utiliser un masque** en regard du champ **Type de contrôleur (PID)** si vous voulez que la règle sélectionnée autorise la connexion de tous les périphériques de stockage de masse conformes aux données indiquées relatives au fabricant et au numéro de série du périphérique.
  - Cochez la case **Utiliser un masque** en regard du champ **Numéro de série** si vous voulez que la règle sélectionnée autorise la connexion de tous les périphériques de stockage de masse conformes aux données indiquées relatives au fabricant du périphérique et au type de contrôleur.
  - Cochez les cases **Utiliser un masque** en regard des champs **Type de contrôleur (PID)** et **Numéro de série** si vous voulez que la règle sélectionnée autorise la connexion de tous les périphériques de stockage de masse conformes aux données indiquées relatives au fabricant du périphérique.

Si la case **Utiliser un masque** est cochée dans un champ au moins, les données des champs dont la case est cochée sont remplacées par \* et ne sont pas prises en compte lors du déclenchement de la règle.

5. Le cas échéant, ajoutez des informations dans le champ **Description** pour expliquer la règle. Par exemple, précisez les périphériques auxquels la règle doit s'appliquer.
6. Cliquez sur le bouton **OK**.

Les paramètres de la règle définis seront enregistrés. La zone d'application des règles sera élargie conformément au masque indiqué du chemin d'accès à l'instance du périphérique.

## Configuration de la tâche Génération des règles du Contrôle des périphériques

► Pour configurer la tâche Génération des règles du Contrôle des périphériques, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Choisissez le nœud enfant **Génération des règles du Contrôle des périphériques**.
3. Dans le panneau de détails du nœud **Génération des règles du Contrôle des périphériques**, cliquez sur le lien **Propriétés**.



La fenêtre **Paramètres de la tâche** s'ouvre.

4. Sous l'onglet **Général**, sélectionnez le mode de fonctionnement de la tâche dans la section **Mode de tâche** :

- **Tenir compte des données du système sur tous les stockages de masse connectés à un moment donné.**
- **Tenir compte des données sur les stockages de masse connectés actuellement.**

5. Dans la section **Une fois la tâche terminée**, indiquez les actions que Kaspersky Security for Windows Server doit réaliser à la fin de la tâche :

- **Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques.**

La case active ou désactive l'ajout des règles d'autorisation créées à la liste des règles du Contrôle des périphériques. La liste des règles du Contrôle des périphériques est affichée via le lien **Règles du Contrôle des périphériques** du volet des détails du nœud **Contrôle des périphériques**.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les règles créées au cours de l'exécution de la tâche Génération des règles du Contrôle des périphériques à la liste de règles du Contrôle des périphériques conformément au principe d'ajout défini.

Si la case est décochée, Kaspersky Security for Windows Server n'ajoute pas les règles d'autorisation créées à la liste de règles du Contrôle des périphériques. Les règles créées sont exportées uniquement dans un fichier.

Cette case est cochée par défaut.

La case ne peut être décochée si la case **Exporter les règles d'autorisation vers un fichier** n'est pas cochée.

- **Principe d'ajout.**

Il s'agit d'une liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications.

- **Ajouter aux règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes.** Les règles remplacent les règles existantes.
- **Fusionner avec les règles existantes.** Les règles sont ajoutée à la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

Le mode **Fusionner avec les règles existantes** est sélectionné par défaut.

- **Exporter les règles d'autorisation vers un fichier.**

La case active ou désactive l'exportation des règles d'autorisation pour le contrôle des périphériques vers un fichier.

Si la case est cochée, Kaspersky Security for Windows Server exporte les règles d'autorisation vers le fichier indiqué dans le champ ci-dessous, une fois la tâche Génération des règles du Contrôle des périphériques terminée.

Quand cette case est décochée, l'application n'exporte pas les règles d'autorisation générées dans un fichier à la fin de la tâche Génération des règles du Contrôle des périphériques. Elle se contente de les ajouter à la liste des règles du Contrôle des périphériques.

Cette case est décochée par défaut.



La case ne peut pas être cochée si la case **Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques** n'est pas cochée.

- **Ajouter des informations sur l'ordinateur dans le nom du fichier.**

La case active ou désactive l'ajout des informations relatives au serveur protégé au nom du fichier dans lequel sont exportées les règles d'autorisation du Contrôle des périphériques

Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur protégé ainsi que la date et l'heure de création du fichier.

Si la case est décochée, l'application n'ajoute pas les informations relatives au serveur protégé dans le nom du fichier d'exportation.

Cette case est cochée par défaut.

6. Les onglets **Planification** et **Avancé** permettent de configurer les paramètres du lancement planifié de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [158](#)).

7. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

# Gestion du pare-feu

Cette section contient des informations sur la tâche Gestion du pare-feu et sa configuration.

## Contenu du chapitre

A propos de la tâche Gestion du pare-feu .....	<a href="#">443</a>
A propos des règles du pare-feu .....	<a href="#">444</a>
Paramètres par défaut de la tâche Gestion du pare-feu .....	<a href="#">446</a>
Administration des règles du pare-feu via le plug-in d'administration .....	<a href="#">446</a>
Administration des règles du pare-feu via la Console de l'application .....	<a href="#">450</a>

## A propos de la tâche Gestion du pare-feu

Kaspersky Security for Windows Server offre une solution fiable et ergonomique pour la protection des connexions réseau grâce à la tâche Gestion du pare-feu.

La tâche Gestion du pare-feu ne réalise pas un filtrage indépendant du trafic réseau, mais il permet d'administrer le pare-feu Windows via l'interface graphique de Kaspersky Security for Windows Server. Au cours de l'exécution de la tâche Gestion du pare-feu, Kaspersky Security for Windows Server assume complètement l'administration des paramètres et des règles du pare-feu du système d'exploitation et interdit toute tentative de configuration de pare-feu externe.

Au cours de l'installation de l'application, le composant Gestion du pare-feu lit et copie l'état du pare-feu Windows, ainsi que toutes les règles définies. Par la suite, la modification de l'ensemble des règles ou de leurs paramètres, ainsi que l'arrêt ou le lancement du pare-feu seront possibles uniquement via Kaspersky Security for Windows Server.

Si le pare-feu Windows est désactivé lors de l'installation de Kaspersky Security for Windows Server, la tâche Gestion du pare-feu n'est pas lancée à la fin de l'installation. Si le pare-feu Windows est activé lors de l'installation de l'application, la tâche Gestion du pare-feu est exécutée à la fin de l'installation et bloque toutes les connexions de réseau sur la base des règles définies autorisées.

Le composant Gestion du pare-feu n'est pas repris dans la sélection de composants de l'installation recommandée et n'est pas installé par défaut.

La tâche Gestion du pare-feu force l'interdiction de toutes les connexions entrantes et sortantes si elles ne sont pas autorisées par les règles définies de la tâche.

La tâche interroge régulièrement le pare-feu Windows et contrôle son état. L'intervalle de sondage par défaut est de 1 minute et il n'est pas modifiable. Si à l'issue de l'interrogation Kaspersky Security for Windows Server détecte un écart entre les paramètres du pare-feu Windows et ceux de la tâche Gestion du pare-feu, l'application impose les

paramètres de la tâche au pare-feu du système d'exploitation.

Lors de l'interrogation du pare-feu Windows qui a lieu toutes les minutes, Kaspersky Security for Windows Server contrôle les éléments suivants :

- état de fonctionnement du pare-feu Windows ;
- l'état de règles ajoutées après l'installation de Kaspersky Security for Windows Server par d'autres applications ou outils (par exemple, ajout d'une nouvelle règle de l'application pour un port/une application à l'aide de wf.msc).

Lors de l'application de nouvelles règles au pare-feu Windows, Kaspersky Security for Windows Server crée un ensemble de règles Kaspersky Security Group dans le composant logiciel enfichable **Pare-feu Windows**. Cet ensemble réunit toutes les règles créées par Kaspersky Security for Windows Server via la tâche Gestion du pare-feu. Les règles qui figurent dans le groupe Kaspersky Security Group ne sont pas contrôlées par l'application lors du sondage toutes les minutes et elles ne sont pas synchronisées automatiquement avec la liste des règles définies dans les paramètres de la tâche Gestion du pare-feu. Le cas échéant, vous pouvez actualiser manuellement les règles de Kaspersky Security.

► *Pour mettre à jour manuellement la liste des règles Kaspersky Security Group,*

redémarrez la tâche Gestion du pare-feu de Kaspersky Security for Windows Server.

Vous pouvez également modifier les règles de Kaspersky Security Group manuellement dans le composant logiciel enfichable **Pare-feu Windows**.

Le lancement de la tâche Gestion du pare-feu est impossible si le pare-feu Windows est administré par une stratégie de groupe Kaspersky Security Center.

## A propos des règles du pare-feu

La tâche Gestion du pare-feu contrôle le filtrage du trafic entrant et sortant à l'aide de règles d'autorisation qui sont imposées au pare-feu Windows lors de l'exécution de la tâche.

Au premier lancement de la tâche, Kaspersky Security for Windows Server lit toutes les règles pour le trafic entrant définies dans les paramètres du pare-feu Windows et les copie dans la tâche Gestion du pare-feu. Par la suite, l'application fonctionne conformément aux algorithmes suivants :

- si une règle est créée, manuellement ou automatiquement suite à l'installation d'une nouvelle application, dans les paramètres du pare-feu Windows, Kaspersky Security for Windows Server supprime cette règle ;
- si une règle existante est supprimée dans les paramètres du pare-feu Windows, Kaspersky Security for Windows Server restaure cette règle après le redémarrage de la tâche.
- si les paramètres d'une règle existante sont modifiés dans les paramètres du pare-feu Windows, Kaspersky Security for Windows Server annule les modifications ;
- si une règle est créée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Security for Windows Server impose cette règle au pare-feu Windows ;
- si une règle existante est supprimée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Security for Windows Server impose la suppression de cette règle dans les paramètres du pare-feu Windows ;

Kaspersky Security for Windows Server ne fonctionne pas avec les règles d'interdiction, ni avec les règles de contrôle du trafic sortant. Au lancement de la tâche Gestion du pare-feu, Kaspersky Security for Windows Server supprime toutes les règles de ce genre dans les paramètres du pare-feu Windows.

Vous pouvez créer, supprimer et modifier les règles de filtrage du trafic entrant.

Vous ne pouvez pas définir une nouvelle règle pour le contrôle du trafic sortant via les paramètres de la tâche Gestion du pare-feu. Toutes les règles du pare-feu définies via Kaspersky Security for Windows Server contrôlent uniquement le trafic réseau entrant.

Vous pouvez utiliser les règles de pare-feu des types suivants :

- Règles pour les applications.
- Règles pour les ports.

### Règles pour les applications

Les règles de ce type autorisent au cas par cas les connexions pour les apps indiquées. Le critère de déclenchement de ces règles est le chemin d'accès au fichier exécutable.

Vous pouvez administrer les règles pour les apps :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le chemin d'accès au fichier exécutable et la zone d'application de la règle.

### Règles pour les ports

Les règles de ce type autorisent les connexions réseau pour les ports et les protocoles indiqués (TCP / UDP). Les critères de déclenchement de ces règles sont le numéro du port et le type de protocole.

Vous pouvez administrer les règles pour les ports :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le numéro de port, le type de protocole et la zone d'application de la règle.

Les règles pour les ports ont une plus grande zone d'action que les règles pour les apps. En autorisant les connexions sur la base de règles pour les ports, vous abaissez le niveau de sécurité du serveur protégé.

## Paramètres par défaut de la tâche Gestion du pare-feu

La tâche Gestion du pare-feu utilise les paramètres par défaut décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 61. Paramètres par défaut de la tâche Gestion du pare-feu

Paramètre	Valeur par défaut	Description
Règles du pare-feu pour l'application	Deux règles par défaut pour l'application activées	Vous pouvez désactiver les règles par défaut ou ajouter de nouvelles règles.
Règles du pare-feu pour les ports	Six règles par défaut pour les ports activées	Vous pouvez désactiver les règles par défaut ou ajouter de nouvelles règles.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Gestion du pare-feu n'est pas lancée automatiquement au démarrage de Kaspersky Security for Windows Server. Vous pouvez configurer la planification du lancement de la tâche.

## Administration des règles du pare-feu via le plug-in d'administration

Cette section explique comment administrer les règles du pare-feu via l'interface de la Console de l'application.

### Dans cette section

Activation et désactivation des règles du pare-feu .....	<a href="#">446</a>
Ajout manuel de règles du pare-feu.....	<a href="#">447</a>
Suppression de règles du pare-feu .....	<a href="#">449</a>

## Activation et désactivation des règles du pare-feu

► Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).

- Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Gestion du pare-feu**.
5. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.  
La fenêtre **Règles du pare-feu** s'ouvre.
6. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
7. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :
  - Si vous voulez qu'une règle inactive soit appliquée, cochez la case à gauche du nom de la règle.  
La règle choisie sera activée.
  - Si vous voulez qu'une règle active ne soit plus appliquée, décochez la case à gauche du nom de la règle.  
La règle choisie sera désactivée.
8. Dans la fenêtre **Règles du pare-feu**, cliquez sur **OK**.
9. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
10. Cliquez sur **OK** dans la fenêtre **Propriétés : <nom de la stratégie>**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

## Ajout manuel de règles du pare-feu

Vous pouvez ajouter ou modifier uniquement les règles pour les applications et les ports. Vous ne pouvez pas ajouter des règles de groupe ou modifier les règles de groupe existantes.

- *Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante, procédez comme suit :*
  1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
  2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
  3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
    - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une

stratégie" à la page [123](#)).

- Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Gestion du pare-feu**.

5. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

La fenêtre **Règles du pare-feu** s'ouvre.

6. En fonction du type de règle que vous souhaitez ajouter, choisissez l'onglet **Applications** ou **Ports** et exécutez une des actions suivantes :

- Pour modifier une règle existante, sélectionnez dans la liste des règles celle dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Modifier**.
- Pour créer une règle, cliquez sur le bouton **Ajouter**.

En fonction du type de la règle à configurer, la fenêtre **Configurer une règle pour un port** ou **Règle pour l'application** s'ouvre.

7. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

- Si vous travaillez avec la règle pour une app, procédez comme suit :
  - a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
  - b. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.  
Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.
  - c. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

- Si vous travaillez avec une règle pour un port, procédez comme suit :
  - a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
  - b. Saisissez dans le champ **Numéro de port** le numéro du port pour lequel l'application autorisera les connexions.
  - c. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.
  - d. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

8. Dans la fenêtre **Règle pour l'application** ou **Configurer une règle pour un port**, cliquez sur le bouton **OK**.
9. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
10. Cliquez sur **OK** dans la fenêtre **Propriétés : <nom de la stratégie>**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

## Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

► Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** dans la sous-section **Gestion du pare-feu**.
5. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.  
La fenêtre **Règles du pare-feu** s'ouvre.
6. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
7. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
8. Cliquez sur le bouton **Supprimer**.  
La règle sélectionnée sera supprimée.
9. Dans la fenêtre **Règles du pare-feu**, cliquez sur **OK**.
10. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
11. Cliquez sur **OK** dans la fenêtre **Propriétés : <nom de la stratégie>**.



Les paramètres définis de la tâche Gestion du pare-feu sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

## Administration des règles du pare-feu via la Console de l'application

Cette section explique comment administrer les règles du pare-feu via l'interface de la Console de l'application.

### Dans cette section

Activation et désactivation des règles du pare-feu .....	<a href="#">450</a>
Ajout manuel de règles du pare-feu.....	<a href="#">451</a>
Suppression de règles du pare-feu .....	<a href="#">452</a>

## Activation et désactivation des règles du pare-feu

► *Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Dans le panneau de détails du nœud **Gestion du pare-feu**, cliquez sur le lien **Règles du pare-feu**.  
La fenêtre **Règles du pare-feu** s'ouvre.
4. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
5. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :
  - Si vous voulez qu'une règle inactive soit appliquée, cochez la case à gauche du nom de la règle.  
La règle choisie sera activée.
  - Si vous voulez qu'une règle active ne soit plus appliquée, décochez la case à gauche du nom de la règle.  
La règle choisie sera désactivée.
6. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

## Ajout manuel de règles du pare-feu

► Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Dans le panneau de détails du nœud **Gestion du pare-feu**, cliquez sur le lien **Règles du pare-feu**.

La fenêtre **Règles du pare-feu** s'ouvre.

4. En fonction du type de règle que vous souhaitez ajouter, choisissez l'onglet **Applications** ou **Ports** et exécutez une des actions suivantes :

- Pour modifier une règle existante, sélectionnez dans la liste des règles celle dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Modifier**.
- Pour créer une règle, cliquez sur le bouton **Ajouter**.

En fonction du type de la règle à configurer, la fenêtre **Configurer une règle pour un port** ou **Règle pour l'application** s'ouvre.

5. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

- Si vous travaillez avec la règle pour une app, procédez comme suit :
  - a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
  - b. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.  
Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.
  - c. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

- Si vous travaillez avec une règle pour un port, procédez comme suit :
  - a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.
  - b. Saisissez dans le champ **Numéro de port** le numéro du port pour lequel l'application autorisera les connexions.
  - c. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.
  - d. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

6. Dans la fenêtre **Règle pour l'application** ou **Configurer une règle pour un port**, cliquez sur le bouton **OK**.
7. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

## Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

► Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle du serveur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Dans le panneau de détails du nœud **Gestion du pare-feu**, cliquez sur le lien **Règles du pare-feu**.  
La fenêtre **Règles du pare-feu** s'ouvre.
4. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
5. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
6. Cliquez sur le bouton **Supprimer**.  
La règle sélectionnée sera supprimée.
7. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

# Moniteur d'intégrité des fichiers

Cette section contient des informations sur le lancement et la configuration de la tâche Moniteur d'intégrité des fichiers.

## Contenu du chapitre

A propos de la tâche Moniteur d'intégrité des fichiers .....	<a href="#">453</a>
A propos des règles de monitoring des opérations sur les fichiers .....	<a href="#">454</a>
Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers .....	<a href="#">456</a>
Administration du Moniteur d'intégrité des fichiers via le plug-in d'administration .....	<a href="#">458</a>
Administration du Moniteur d'intégrité des fichiers via la Console de l'application .....	<a href="#">462</a>

## A propos de la tâche Moniteur d'intégrité des fichiers

La tâche Moniteur d'intégrité des fichiers permet de surveiller les actions exécutées sur les fichiers et les dossiers indiqués au sein des zones de monitoring définies dans les paramètres de la tâche. Vous pouvez utiliser la tâche pour détecter les modifications des fichiers afin d'identifier une violation de la sécurité sur le serveur protégé. Il est également possible de configurer le suivi des modifications des fichiers pendant la durée d'interruption du monitoring.

L'*interruption du monitoring* désigne une période au cours de laquelle la zone de monitoring est exclue temporairement de la zone d'action de la tâche, par exemple suite à l'arrêt de la tâche ou en l'absence physique d'un périphérique de stockage de masse sur le serveur protégé. Kaspersky Security for Windows Server signale la détection d'opérations sur les fichiers dans la zone de monitoring dès que le périphérique de stockage de masse est à nouveau connecté.

Une suspension de l'exécution de la tâche dans la zone de monitoring définie suite à la réinstallation du composant Moniteur d'intégrité des fichiers ne constitue pas une interruption du monitoring. Dans ce cas, la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

### Exigences applicables à l'environnement

Pour permettre le lancement de la tâche Moniteur d'intégrité des fichiers, les conditions suivantes doivent être remplies :

- Un périphérique de stockage de masse, compatible avec les systèmes de fichiers ReFS et NTFS, doit être installé sur le serveur protégé.
- Le journal USN Windows doit être activé. Le composant interroge ce journal afin d'obtenir des informations sur les opérations sur les fichiers.

Si vous avez activé le journal USN après que vous avez créé une règle pour un volume et lancé la tâche Moniteur d'intégrité des fichiers, il faut relancer la tâche. Dans le cas contraire, cette règle n'est pas prise en compte par le monitoring.

### Exclusions pour la zone de monitoring

Vous pouvez créer des exclusions pour les zones de monitoring (cf. section "Configuration des règles de monitoring" à la page 459). Les exclusions sont définies pour chaque règle distincte et fonctionnent uniquement pour la zone de monitoring indiquée. Vous pouvez définir un nombre illimité d'exclusions pour chaque règle.

Les exclusions possèdent une priorité plus grande dans la zone de monitoring et elles ne sont pas contrôlées par la tâche, même si un dossier ou fichier indiqué se trouve dans la zone de monitoring. Si les paramètres d'une des règles définissent une zone de monitoring à un niveau inférieur à celui du dossier défini dans les exclusions, la zone de monitoring n'est pas prise en compte quand la tâche est exécutée.

Pour définir les exclusions, il convient d'utiliser les mêmes masques que ceux utilisés pour déterminer la zone de monitoring.

## A propos des règles de monitoring des opérations sur les fichiers

La tâche Moniteur d'intégrité des fichiers est exécutée sur la base de règles de monitoring des opérations sur les fichiers. Les critères de déclenchement de la règle permettent de configurer les conditions de déclenchement d'une tâche et de régler le niveau d'importance des événements pour les opérations réalisées sur les fichiers qui ont été détectées et consignées dans le journal d'exécution de la tâche.

La règle de monitoring des opérations sur les fichiers est définie pour chaque zone de monitoring.

Vous pouvez configurer les critères de déclenchement de la règle suivants :

- Utilisateurs de confiance
- Marqueurs d'opérations sur les fichiers.

### Utilisateurs de confiance

L'application considère par défaut les actions de tous les utilisateurs comme des violations potentielles de la sécurité. La liste des utilisateurs de confiance est vide. Vous pouvez configurer le niveau d'importance de l'événement en dressant une liste d'utilisateurs de confiance dans les paramètres de la règle de monitoring des opérations sur les fichiers.

Un *utilisateur bloqué* désigne n'importe quel utilisateur qui ne figure pas dans la liste des utilisateurs de confiance définie dans les paramètres de la zone de monitoring. Si Kaspersky Security for Windows Server détecte une opération sur un fichier réalisée par un utilisateur bloqué, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance Événement critique dans le journal d'exécution de la tâche.

L'*utilisateur de confiance* est un utilisateur ou un groupe d'utilisateurs autorisé à exécuter des opérations sur les fichiers dans la zone de monitoring indiquée. Si Kaspersky Security for Windows Server détecte une opération sur un fichier réalisée par un utilisateur de confiance, la tâche Moniteur d'intégrité des fichiers consigne l'événement

avec le niveau d'importance Événement d'information dans le journal d'exécution de la tâche.

Kaspersky Security for Windows Server ne peut pas identifier l'utilisateur à l'origine des opérations quand celles-ci ont lieu dans la durée d'interruption du monitoring. Dans ce cas, l'état de l'utilisateur est défini comme inconnu.

L'*utilisateur inconnu* est un état attribué à un utilisateur quand Kaspersky Security for Windows Server ne peut pas recevoir les données relatives à l'utilisateur suite à une interruption de la tâche ou à un échec du pilote de synchronisation des données et du journal USN. Si Kaspersky Security for Windows Server détecte une opération sur un fichier réalisée par un utilisateur inconnu, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance *Avertissement* dans le journal d'exécution de la tâche.

### Marqueurs d'opérations sur les fichiers

Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Security for Windows Server utilise les marqueurs d'opérations sur les fichiers pour confirmer si une action a été réalisée sur le fichier.

Le marqueur d'opération sur les fichiers est un indice unique qui permet de définir une opération réalisée sur un fichier.

Chaque opération réalisée sur un fichier peut être composée d'une seule action ou d'une série d'actions exécutées sur les fichiers. Chaque action de ce genre reçoit un marqueur d'opérations sur les fichiers. Quand un marqueur que vous avez désigné comme critère de déclenchement de la règle de monitoring est détecté dans la chaîne d'opérations réalisées sur un fichier, l'application consigne l'événement lié à la réalisation d'une telle action.

Le niveau d'importance des événements consignés ne dépend pas des marqueurs d'opérations sur les fichiers choisis, ni de leur quantité.

Par défaut, Kaspersky Security for Windows Server tient compte de tous les marqueurs d'opérations sur les fichiers disponibles. Vous pouvez sélectionner les marqueurs d'opérations sur les fichiers manuellement dans les paramètres des règles de la tâche (cf. tableau ci-dessous).

Tableau 62. Marqueurs d'opérations sur les fichiers

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
BASIC_INFO_CHANGE	attributs ou horodatage d'un fichier ou d'un dossier modifiés	NTFS, ReFS
COMPRESSION_CHANGE	compression d'un fichier ou d'un dossier modifiée	NTFS, ReFS
DATA_EXTEND	taille du fichier ou du dossier augmentée	NTFS, ReFS
DATA_OVERWRITE	Données dans le fichier ou me dossier écrasées	NTFS, ReFS
DATA_TRUNCATION	fichier ou dossier tronqués	NTFS, ReFS
EA_CHANGE	attributs étendus du fichier ou du dossier modifiés	NTFS uniquement
ENCRYPTION_CHANGE	état de chiffrement malveillant du fichier ou du dossier modifié	NTFS, ReFS

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
FILE_CREATE	fichier ou dossier créés pour la première fois	NTFS, ReFS
FILE_DELETE	Fichier ou dossier supprimé définitivement par une combinaison MAJ+SUPPR	NTFS, ReFS
HARD_LINK_CHANGE	lien physique pour le fichier ou le dossier créé ou supprimé	NTFS uniquement
INDEXABLE_CHANGE	état d'indexation du fichier ou du dossier modifié	NTFS, ReFS
INTEGRITY_CHANGE	attribut d'intégrité pour le flux de fichiers nommé modifié	ReFS uniquement
NAMED_DATA_EXTEND	taille du flux de fichiers nommé augmentée	NTFS, ReFS
NAMED_DATA_OVERWRITE	flux de fichiers nommé écrasé	NTFS, ReFS
NAMED_DATA_TRUNCATION	flux de fichiers nommé tronqué	NTFS, ReFS
OBJECT_ID_CHANGE	identifiant de fichier ou de dossier modifié	NTFS, ReFS
RENAME_NEW_NAME	nouveau nom attribué au fichier ou au dossier	NTFS, ReFS
REPARSE_POINT_CHANGE	point d'analyse répétée pour le fichier ou le dossier créé ou point d'analyse répétée existant modifié	NTFS, ReFS
SECURITY_CHANGE	autorisations d'accès au fichier ou au dossier modifiées	NTFS, ReFS
STREAM_CHANGE	flux de fichier nommé créé ou flux existant modifié	NTFS, ReFS
TRANSACTION_CHANGE	flux de fichier nommé modifié par la transaction TxF	ReFS uniquement

## Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

La tâche Moniteur d'intégrité des fichiers possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 63. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
<b>Zone de monitoring</b>	Non configuré	Vous pouvez définir les dossiers et les fichiers pour lesquels les opérations doivent être surveillées. Des événements de monitoring sont créés pour les dossiers et les fichiers de la zone de monitoring définie.
<b>Liste des utilisateurs de confiance</b>	Non configuré	Vous pouvez désigner des utilisateurs et/ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.
<b>Contrôler les opérations sur les fichiers pendant la pause de la tâche</b>	Appliquée	Vous pouvez activer ou désactiver l'enregistrement des opérations réalisées sur les fichiers dans les zones de monitoring indiquées pendant la durée d'interruption de la tâche.
<b>Exclure les dossiers suivants du contrôle</b>	Pas appliqué	Vous pouvez contrôler l'application des exclusions pour les dossiers où il n'est pas nécessaire de surveiller les opérations réalisées sur les fichiers. Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Security for Windows Server ignore les zones de monitoring définies en tant qu'exclusion.
<b>Calcul de la somme de contrôle</b>	Pas appliqué	Vous pouvez configurer le calcul de la somme de contrôle d'un fichier après que des modifications ont été introduites dans celui-ci.
<b>Tenir compte des marqueurs d'opérations sur les fichiers</b>	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Vous pouvez définir un ensemble de marqueurs pour caractériser les opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de monitoring se caractérise par au moins un des marqueurs indiqués, Kaspersky Security for Windows Server génère un événement d'audit.
<b>Planification du lancement de la tâche</b>	Le premier lancement n'est pas défini	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.



# Administration du Moniteur d'intégrité des fichiers via le plug-in d'administration

Cette section explique comment configurer le Moniteur d'intégrité des fichiers via le plug-in d'administration.

## Dans cette section

Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers.....	<a href="#">458</a>
Configuration des règles de monitoring.....	<a href="#">459</a>

## Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers

Pour configurer les paramètres généraux de la tâche Moniteur d'intégrité des fichiers, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** du groupe **Moniteur d'intégrité des fichiers**, cliquez sur le bouton **Configuration**.

La fenêtre **Moniteur d'intégrité des fichiers** s'ouvre.

5. Sous l'onglet **Paramètres de monitoring des opérations sur les fichiers** de la fenêtre qui s'ouvre, configurez les paramètres de la zone de monitoring :
  - a. Cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du monitoring**.

La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

Si la case est cochée, Kaspersky Security for Windows Server consigne les événements survenus dans toutes les zones de monitoring quand la tâche Moniteur d'intégrité des

fichiers n'est pas exécutée.

Si la case est décochée, les opérations sur les fichiers journaux réalisées dans les zones de monitoring pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

Cette case est cochée par défaut.

- b. Ajoutez les zones de monitoring (cf. section "Configuration des règles de monitoring" à la page [459](#)) que la tâche va surveiller
6. Sous l'onglet **Administration des tâches**, configurez les paramètres de lancement de la tâche selon une planification (cf. section "Programmation des tâches" à la page [138](#)).
7. Cliquez sur le bouton **OK** pour enregistrer les modifications.

## Configuration des règles de monitoring

Vous pouvez modifier les paramètres de la tâche Moniteur d'intégrité des fichiers précisés par défaut (cf. tableau ci-dessous).

Tableau 64. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
<b>Zone de monitoring</b>	Non configuré	Vous pouvez définir les dossiers et les fichiers pour lesquels les opérations doivent être surveillées. Des événements de monitoring sont créés pour les dossiers et les fichiers de la zone de monitoring définie.
<b>Liste des utilisateurs de confiance</b>	Non configuré	Vous pouvez désigner des utilisateurs et/ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.
<b>Contrôler les opérations sur les fichiers pendant la pause de la tâche</b>	Appliquée	Vous pouvez activer ou désactiver l'enregistrement des opérations réalisées sur les fichiers dans les zones de monitoring indiquées pendant la durée d'interruption de la tâche.
<b>Exclure les dossiers suivants du contrôle</b>	Pas appliqué	Vous pouvez contrôler l'application des exclusions pour les dossiers où il n'est pas nécessaire de surveiller les opérations réalisées sur les fichiers. Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Security for Windows Server ignore les zones de monitoring définies en tant qu'exclusion.
<b>Calcul de la somme de contrôle</b>	Pas appliqué	Vous pouvez configurer le calcul de la somme de contrôle d'un fichier après que des modifications ont été introduites dans celui-ci.
<b>Tenir compte des marqueurs d'opérations sur les fichiers</b>	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Vous pouvez définir un ensemble de marqueurs pour caractériser les opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de monitoring se caractérise par au moins un des marqueurs indiqués, Kaspersky Security for Windows Server génère un événement d'audit.

Paramètre	Valeur par défaut	Description
<b>Planification du lancement de la tâche</b>	Le premier lancement n'est pas défini	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

► Pour ajouter une zone de monitoring, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** du groupe **Moniteur d'intégrité des fichiers**, cliquez sur le bouton **Configuration**.  
La fenêtre **Propriétés : Moniteur d'intégrité des fichiers** s'ouvre.
5. Dans la section **Zone de monitoring**, cliquez sur le bouton **Ajouter**.  
La fenêtre **Zone de monitoring** s'ouvre.
6. Ajoutez une zone de monitoring à l'aide d'une des méthodes suivantes :
  - Si vous voulez choisir les dossiers via la boîte de dialogue Microsoft Windows standard :
    - a. Cliquez sur le bouton **Parcourir**.  
La fenêtre standard de Microsoft Windows Parcourir le dossier s'ouvre.
    - b. Dans la fenêtre qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations, puis cliquez sur le bouton **OK**.
  - Si vous voulez définir la zone de monitoring manuellement, ajoutez le chemin d'accès à l'aide d'un des masques pris en charge :
    - `<*.ext>` : tous les fichiers avec l'extension `<ext>`, quel que soit leur emplacement ;
    - `<*\name.ext>` : tous les fichiers portant le nom `name` et l'extension `<ext>`, quel que soit leur emplacement ;
    - `<\dir\*>` : tous les fichiers du dossier `<\dir>` ;
    - `<\dir\*\name.ext>` : tous les fichiers portant le nom `<name>` et l'extension `<ext>` dans le dossier `<\dir>` et l'ensemble de ses sous-dossiers.

Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque>. En l'absence de l'indication du volume, Kaspersky Security for Windows Server n'ajoute pas la zone de monitoring indiquée.

7. Sous l'onglet **Utilisateurs de confiance**, cliquez sur le bouton **Ajouter**.

La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

8. Sélectionnez les utilisateurs ou groupes d'utilisateurs autorisés à exécuter des opérations sur les fichiers dans la zone de monitoring sélectionnée, puis cliquez sur **OK**.

Kaspersky Security for Windows Server considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs bloqué (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page 454) et génère pour ceux-ci des événements de niveau Critique.

9. Choisissez l'onglet **Marqueurs d'opérations sur les fichiers**.

10. Le cas échéant, sélectionnez plusieurs marqueurs d'opération sur les fichiers en réalisant les opérations suivantes :

- Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.
- Dans la liste des opérations sur les fichiers disponibles qui s'ouvre (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page 454), cochez les cases en regard des opérations que vous souhaitez contrôler.

Kaspersky Security for Windows Server détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

11. Si vous souhaitez que Kaspersky Security for Windows Server calcule la somme de contrôle des fichiers après l'opération, procédez comme suit :

- Cochez la case **Calculer la somme de contrôle du fichier si possible. Elle sera reprise dans le rapport de la tâche**.

Si la case est cochée, Kaspersky Security for Windows Server calcule la somme de contrôle du fichier modifié dans lequel une opération correspondant à au moins un marqueur sélectionné a été détectée.

Si l'opération sur le fichier est détectée à l'aide de plusieurs marqueurs, seule la somme de contrôle finale est calculée après la totalité des modifications.

Si la case est décochée, Kaspersky Security for Windows Server ne calcule pas la somme de contrôle pour les fichiers modifiés.

Aucune somme de contrôle n'est calculée dans les cas suivants :

- si le fichier est devenu inaccessible (par exemple, modification des autorisations d'accès au fichier) ;
- si l'opération réalisée sur le fichier concerne un fichier qui a été supprimé par la suite.

Cette case est décochée par défaut.

- Sélectionnez une des options de la liste déroulante **Calculer la somme de contrôle selon**

**l'algorithme :**

- **Hash MD5**
- **Hash SHA256**

12. Si vous ne souhaitez pas contrôler la totalité des opérations exécutées sur les fichiers, ouvrez la liste des opérations sur les fichiers disponibles (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page [454](#)) et cochez les cases en regard des opérations que vous souhaitez contrôler.

13. Le cas échéant, ajoutez des exclusions pour la zone de monitoring de la manière suivante :

- Sélectionnez l'onglet **Exclusions**.
- Cochez la case **Exclure les dossiers suivants du contrôle**.

La case désactive l'application des exclusions pour les dossiers dans lesquels il n'est pas nécessaire de contrôler les opérations sur les fichiers.

Si la case est cochée, Kaspersky Security for Windows Server ignore les zones de monitoring reprises dans la liste des exclusions lors de l'exécution de la tâche Moniteur d'intégrité des fichiers.

Si la case est décochée, Kaspersky Security for Windows Server enregistre les événements pour toutes les zones de monitoring définies.

La case est décochée par défaut, la liste des exclusions est vide.

- Cliquez sur **Ajouter**.

La fenêtre **Sélectionnez un dossier à ajouter** s'ouvre.

- Dans la fenêtre qui s'ouvre, sélectionnez le dossier que vous souhaitez exclure de la zone de monitoring.

- Cliquez sur le bouton **OK**.

Le dossier indiqué est ajouté à la liste des zones exclues.

14. Cliquez sur **OK** dans la fenêtre **Règle de monitoring des opérations sur les fichiers**.

Les paramètres définis pour la règle seront appliqués à la zone de monitoring sélectionnée de la tâche Moniteur d'intégrité des fichiers.

## Administration du Moniteur d'intégrité des fichiers via la Console de l'application

Cette section explique comment configurer le Moniteur d'intégrité des fichiers via la Console de l'application.

### Dans cette section

Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers.....	<a href="#">463</a>
Configuration des règles de monitoring.....	<a href="#">463</a>

## Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers

► Pour configurer les paramètres généraux de la tâche Moniteur d'intégrité des fichiers, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Moniteur d'intégrité des fichiers**.
3. Dans le panneau de détails du nœud **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Propriétés**. La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Général**, puis cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du monitoring**.

La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

Si la case est cochée, Kaspersky Security for Windows Server consigne les événements survenus dans toutes les zones de monitoring quand la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

Si la case est décochée, les opérations sur les fichiers journaux réalisées dans les zones de monitoring pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

Cette case est cochée par défaut.

5. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section "Programmation des tâches" à la page [138](#)).
6. Cliquez sur le bouton **OK** pour enregistrer les modifications.

## Configuration des règles de monitoring

Vous pouvez modifier les paramètres de la tâche Moniteur d'intégrité des fichiers précisés par défaut (cf. tableau ci-dessous).

Tableau 65. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
<b>Zone de monitoring</b>	Non configuré	Vous pouvez définir les dossiers et les fichiers pour lesquels les opérations doivent être surveillées. Des événements de monitoring sont créés pour les dossiers et les fichiers de la zone de monitoring définie.
<b>Liste des utilisateurs de confiance</b>	Non configuré	Vous pouvez désigner des utilisateurs et/ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.

Paramètre	Valeur par défaut	Description
<b>Contrôler les opérations sur les fichiers pendant la pause de la tâche</b>	Appliquée	Vous pouvez activer ou désactiver l'enregistrement des opérations réalisées sur les fichiers dans les zones de monitoring indiquées pendant la durée d'interruption de la tâche.
<b>Exclure les dossiers suivants du contrôle</b>	Pas appliqué	Vous pouvez contrôler l'application des exclusions pour les dossiers où il n'est pas nécessaire de surveiller les opérations réalisées sur les fichiers. Lors de l'exécution de la tâche <b>Moniteur d'intégrité des fichiers</b> , Kaspersky Security for Windows Server ignore les zones de monitoring définies en tant qu'exclusion.
<b>Calcul de la somme de contrôle</b>	Pas appliqué	Vous pouvez configurer le calcul de la somme de contrôle d'un fichier après que des modifications ont été introduites dans celui-ci.
<b>Tenir compte des marqueurs d'opérations sur les fichiers</b>	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Vous pouvez définir un ensemble de marqueurs pour caractériser les opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de monitoring se caractérise par au moins un des marqueurs indiqués, Kaspersky Security for Windows Server génère un événement d'audit.
<b>Planification du lancement de la tâche</b>	Le premier lancement n'est pas défini	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

► *Pour ajouter une zone de monitoring, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Moniteur d'intégrité des fichiers**.
3. Dans le panneau de détails du nœud **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Règles de monitoring des opérations sur les fichiers**.

La fenêtre **Monitoring des opérations sur les fichiers** s'ouvre.

4. Ajoutez une zone de monitoring à l'aide d'une des méthodes suivantes :
  - Si vous voulez choisir les dossiers via la boîte de dialogue Microsoft Windows standard :
    - a. Dans la partie gauche de la fenêtre, cliquez sur le bouton **Parcourir**.  
La fenêtre standard de Microsoft Windows **Parcourir le dossier** s'ouvre.
    - b. Dans la fenêtre qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations, puis cliquez sur le bouton **OK**.
    - c. Cliquez sur le bouton **Ajouter** pour que Kaspersky Security for Windows Server commence à contrôler les opérations sur les fichiers dans la zone de monitoring indiquée.
  - Si vous voulez définir la zone de monitoring manuellement, ajoutez le chemin d'accès à l'aide d'un des masques pris en charge :
    - `<*.ext>` : tous les fichiers avec l'extension `<ext>`, quel que soit leur emplacement ;
    - `<*\name.ext>` : tous les fichiers portant le nom `name` et l'extension `<ext>`, quel que soit leur



emplacement ;

- <dir\\*> : tous les fichiers du dossier <dir> ;
- <dir\\*\name.ext> : tous les fichiers portant le nom <name> et l'extension <ext> dans le dossier <dir> et l'ensemble de ses sous-dossiers.

Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque>. En l'absence de l'indication du volume, Kaspersky Security for Windows Server n'ajoute pas la zone de monitoring indiquée.

Dans la partie droite de la fenêtre, l'onglet **Description** affiche les utilisateurs de confiance et les marqueurs d'opérations sur les fichiers sélectionnés pour cette zone de monitoring.

5. Dans la liste des zones de monitoring ajoutées, sélectionnez celle pour laquelle vous souhaitez configurer d'autres paramètres.
6. Ouvrez l'onglet **Utilisateurs de confiance**.
7. Cliquez sur **Ajouter**.

La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

8. Choisissez les utilisateurs ou les groupes d'utilisateurs considérés que Kaspersky Security for Windows Server considère comme étant de confiance pour la zone de monitoring sélectionnée.
9. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs bloqué (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page [454](#)) et génère pour ceux-ci des événements de niveau Critique.

10. Choisissez l'onglet **Définir les marqueurs d'opérations sur les fichiers**.
11. Le cas échéant, sélectionnez plusieurs marqueurs d'opération sur les fichiers en réalisant les opérations suivantes :
  - a. Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.
  - b. Dans la liste des opérations sur les fichiers disponibles qui s'ouvre (cf. section "A propos des règles de monitoring des opérations sur les fichiers" à la page [454](#)), cochez les cases en regard des opérations que vous souhaitez contrôler.

Kaspersky Security for Windows Server détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

12. Si vous souhaitez que Kaspersky Security for Windows Server calcule la somme de contrôle des fichiers après l'opération, procédez comme suit :
  - a. Dans la section **Calcul de la somme de contrôle**, cochez la case **Calculer, si possible, la somme de contrôle du fichier modifié**.

Si la case est cochée, Kaspersky Security for Windows Server calcule la somme de contrôle du fichier modifié dans lequel une opération correspondant à au moins un



marqueur sélectionné a été détectée.

Si l'opération sur le fichier est détectée à l'aide de plusieurs marqueurs, seule la somme de contrôle finale est calculée après la totalité des modifications.

Si la case est décochée, Kaspersky Security for Windows Server ne calcule pas la somme de contrôle pour les fichiers modifiés.

Aucune somme de contrôle n'est calculée dans les cas suivants :

- si le fichier est devenu inaccessible (par exemple, modification des autorisations d'accès au fichier) ;
- si l'opération réalisée sur le fichier concerne un fichier qui a été supprimé par la suite.

Cette case est décochée par défaut.

- b. Sélectionnez une des options de la liste déroulante **Calculer la somme de contrôle selon l'algorithme** :

- **Hash MD5.**
- **Hash SHA256.**

13. Le cas échéant, ajoutez des exclusions pour la zone de monitoring de la manière suivante :

- a. Sélectionnez l'onglet **Définir les exclusions**.
- b. Cochez la case **Tenir compte de la zone de monitoring exclue**.

La case désactive l'application des exclusions pour les dossiers dans lesquels il n'est pas nécessaire de contrôler les opérations sur les fichiers.

Si la case est cochée, Kaspersky Security for Windows Server ignore les zones de monitoring reprises dans la liste des exclusions lors de l'exécution de la tâche Moniteur d'intégrité des fichiers.

Si la case est décochée, Kaspersky Security for Windows Server enregistre les événements pour toutes les zones de monitoring définies.

La case est décochée par défaut, la liste des exclusions est vide.

- c. Cliquez sur le bouton **Parcourir**.

La fenêtre standard de Microsoft Windows **Parcourir le dossier** s'ouvre.

- d. Dans la fenêtre qui s'ouvre, sélectionnez le dossier que vous souhaitez exclure de la zone de monitoring.
- e. Cliquez sur le bouton **OK**.
- f. Cliquez sur **Ajouter**.

Le dossier indiqué est ajouté à la liste des zones exclues.

**Vous pouvez également ajouter des exclusions pour la zone de monitoring manuellement en utilisant les masques identiques à ceux employés pour définir les zones de monitoring.**

14. Cliquez sur le bouton **Enregistrer** pour appliquer la nouvelle configuration de règle.

# Inspection des journaux

Cette section contient des informations sur la tâche Inspection des journaux et la configuration de ses paramètres.

## Contenu du chapitre

A propos de la tâche Inspection des journaux.....	<a href="#">467</a>
Paramètres de la tâche Inspection des journaux par défaut .....	<a href="#">468</a>
Administration des règles d'inspection des journaux via le plug-in d'administration .....	<a href="#">469</a>
Administration des règles d'inspection des journaux via la Console de l'application .....	<a href="#">472</a>

## A propos de la tâche Inspection des journaux

Au cours de l'exécution de la tâche Inspection des journaux, Kaspersky Security for Windows Server contrôle l'intégrité de l'environnement protégé d'après les résultats de l'inspection des journaux des événements Windows. L'application informe l'administrateur en cas de détection de signes de comportement atypique dans le système pouvant indiquer des tentatives d'attaques informatiques.

Kaspersky Security for Windows Server tient compte des données des journaux des événements Windows et définit les violations conformément aux règles précisées par l'utilisateur ou par les paramètres de l'analyse heuristique, appliqués par la tâche d'inspection des journaux.

### Règles prédéfinie et analyse heuristique

Vous pouvez utiliser la tâche Inspection des journaux pour contrôler l'état du système protégé en appliquant les règles prédéfinies sur la base des heuristiques prédéterminées. L'analyseur heuristique définit la présence d'une activité anormale sur le serveur protégé, ce qui peut être le signe d'une tentative d'attaque. Les modèles de définition d'une activité anormale sont repris dans les règles disponibles dans les paramètres de règles prédéfinies.

La liste des règles de la tâche Inspection des journaux répertorie sept règles. Vous pouvez activer et désactiver l'application de n'importe quelle règle. Vous ne pouvez pas supprimer de règles existantes ou en créer de nouvelles.

Vous pouvez configurer les critères de déclenchement des règles qui contrôlent les événements pour les opérations suivantes :

- Détection des attaques brute-force
- Traitement de la connexion au réseau

Dans les paramètres de la tâche, vous pouvez configurer également les exclusions. L'analyseur heuristique ne fonctionne pas si l'accès au système est exécuté par un utilisateur de confiance ou via une adresse IP de confiance.

**Kaspersky Security for Windows Server n'applique pas l'heuristique à l'inspection des journaux Windows si l'analyseur heuristique n'est pas utilisé par la tâche. Par défaut, l'analyseur heuristique est activé.**

Lors de l'application des règles, l'application consigne un événement avec le niveau d'importance *Critique* dans le journal d'exécution de la tâche Inspection des journaux.

## Règles personnalisées de la tâche Inspection des journaux

A l'aide des paramètres des règles de la tâche, vous pouvez préciser et modifier les critères de déclenchement de la règle en cas de détection des événements choisis dans le journal Windows indiqué. Par défaut, la liste des règles de la tâche Inspection des journaux contient quatre règles. Vous pouvez activer et désactiver l'application de ces règles, supprimer les règles et en modifier les paramètres.

Vous pouvez configurer les critères suivants de déclenchement de chaque règle :

- Liste des identificateurs des enregistrements dans le journal des événements Windows.

La règle se déclenche à l'apparition d'un nouvel enregistrement dans le journal des événements Windows, si dans les paramètres de l'événement, l'identificateur de l'événement indiqué dans la règle est détecté. Vous pouvez ajouter et supprimer aussi des identificateurs pour chaque règle précisée.

- Source des événements.

Pour chaque règle, vous pouvez préciser un sous-journal du journal des événements Windows. L'application exécutera la recherche des enregistrements avec les identificateurs d'événements indiqués seulement dans ce sous-journal. Vous pouvez sélectionner un des journaux secondaires standard (Application, Sécurité ou Système) ou définir un journal secondaire personnalisé en saisissant le nom dans le champ de sélection de la source.

L'application ne contrôle pas la présence réelle du sous-journal indiqué dans le journal des événements Windows.

Quand la règle est déclenchée, Kaspersky Security for Windows Server enregistre un événement Critique dans le journal d'exécution de la tâche d'inspection des journaux.

Par défaut, la tâche Inspection des journaux ne prend pas en charge les règles personnalisées.

Avant de démarrer la tâche Inspection des journaux, assurez-vous que la stratégie d'audit système est correctement configurée. Consultez l'article de Microsoft (<https://technet.microsoft.com/en-us/library/cc952128.aspx>) pour plus de détails.

## Paramètres de la tâche Inspection des journaux par défaut

La tâche Inspection des journaux possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 66. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
Inspecter les journaux selon les règles personnalisées	Appliquée.	Vous pouvez activer, désactiver, ajouter ou modifier des règles personnalisées.
Appliquer des règles prédéfinies à l'inspection des journaux	Appliquée.	Vous pouvez activer ou désactiver l'analyse heuristique qui détecte l'activité anormale sur le serveur protégé.

Paramètre	Valeur par défaut	Description
Détection des attaques brute-force	10 échecs de connexion toutes les 300 secondes.	Vous pouvez définir le nombre de tentatives et l'intervalle d'exécution de celles-ci qui vont servir de critères de déclenchement de l'analyse heuristique.
Connexion au réseau	00:00:00	Vous pouvez indiquer le début et la fin de l'intervalle de temps pendant lequel Kaspersky Security for Windows Server traite les tentatives d'ouverture de session comme une activité anormale.
Exclusions	Pas appliqué.	Vous pouvez spécifier les utilisateurs et les adresses IP qui ne déclencheront pas l'analyse heuristique.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

## Administration des règles d'inspection des journaux via le plug-in d'administration

Cette section explique comment ajouter des règles d'inspection des journaux et les configurer via le Plug-in d'administration

### Dans cette section

Administration des règles de tâches prédéfinies via le plug-in d'administration .....	<a href="#">469</a>
Ajout de règles d'inspection des journaux via le plug-in d'administration .....	<a href="#">471</a>

## Administration des règles de tâches prédéfinies via le plug-in d'administration

- *Pour configurer les règles prédéfinies de la tâche Inspection des journaux, procédez comme suit :*
1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
  2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
  3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
    - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).

- Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** du groupe **Inspection des journaux**, cliquez sur le bouton **Configuration**.

La fenêtre **Inspection des journaux** s'ouvre.

5. Sélectionnez l'onglet **Règles prédéfinies**.
6. Cochez ou décochez la case **Inspecter les journaux selon les règles personnalisées**.

Si cette case est cochée, Kaspersky Security for Windows Server applique l'analyse heuristique pour détecter toute activité anormale sur le serveur protégé.

Si cette case n'est pas cochée, l'analyse heuristique est désactivée, Kaspersky Security for Windows Server utilise les règles prédéfinies ou définies par l'utilisateur pour détecter les activités anormales.

Cette case est cochée par défaut.

Pour que la tâche fonctionne, il faut sélectionner au moins une règle d'inspection des journaux.

7. Sélectionnez les éléments heuristiques que vous souhaitez appliquer à l'inspection des journaux dans la liste des éléments disponibles :
  - Tentative d'attaque brute-force dans le système.
  - Des signes d'abus potentiel du journal des événements Windows ont été détectés.
  - Des actions suspectes émanant d'un nouveau service installé ont été détectées.
  - Une authentification suspecte avec des identifiants explicites a été détectée.
  - Le système affiche les signes d'une éventuelle attaque Kerberos forged PAC (MS14-068).
  - Des actions suspectes contre un groupe Administrateurs privilégié intégré ont été détectées.
  - Une activité suspecte a été détectée lors d'une session de connexion au réseau.
8. Pour configurer les règles sélectionnées, cliquez sur le bouton **Paramètres avancés**.

La fenêtre **Inspection des journaux** s'ouvre.
9. Dans la section **Détection des attaques brute-force**, définissez le nombre de tentatives et l'intervalle d'exécution de celles-ci qui vont servir de critères de déclenchement de l'analyse heuristique.
10. Dans la section **Détection de la connexion au réseau**, définissez le début et la fin de l'intervalle de temps pendant lequel Kaspersky Security for Windows Server considère les tentatives de connexion comme une activité anormale.
11. Sélectionnez l'onglet **Exclusions**.
12. Pour ajouter des utilisateurs considérés comme des utilisateurs de confiance, procédez comme suit :
  - a. Cliquez sur le bouton **Parcourir**.

- b. Choisissez l'utilisateur.
- c. Cliquez sur le bouton **OK**.

L'utilisateur indiqué est ajouté à la liste des utilisateurs de confiance.

13. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :

- a. Saisissez l'adresse IP.
- b. Cliquez sur **Ajouter**.

14. L'adresse IP indiquée est ajoutée à la liste des adresses de confiance.

15. L'onglet **Administration des tâches** permet de planifier le lancement de la tâche (cf. section "Configuration des paramètres de la planification du lancement de la tâche" à la page [138](#)).

16. Cliquez sur le bouton **OK**.

Les paramètres de la tâche Inspection des journaux sont enregistrés.

## Ajout de règles d'inspection des journaux via le plug-in d'administration

► *Pour ajouter et configurer une nouvelle règle d'inspection des journaux définies par l'utilisateur, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
  - Pour configurer les paramètres de l'application pour un groupe de serveurs, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** (cf. section "Configuration d'une stratégie" à la page [123](#)).
  - Afin de configurer l'application pour un seul serveur, sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application** (cf. section "Configuration des tâches locales dans la fenêtre Paramètres de l'application dans Kaspersky Security Center" à la page [127](#)).

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil, et si la stratégie interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** du groupe **Inspection des journaux**, cliquez sur le bouton **Configuration**.

La fenêtre **Inspection des journaux** s'ouvre.

5. Sous l'onglet **Règles personnalisées**, décochez ou cochez la case **Inspecter les journaux selon les règles personnalisées**.

Si cette case est cochée, Kaspersky Security for Windows Server applique les règles définies par l'utilisateur pour l'inspection des journaux conformément aux paramètres de chaque règle. Vous pouvez ajouter, supprimer ou configurer des règles d'inspection des journaux.

Si la case est décochée, vous ne pouvez pas ajouter de règles personnalisées ni en modifier. Kaspersky Security for Windows Server applique les paramètres de règles par défaut.

Cette case est cochée par défaut. Seule la règle de détection de pop-up d'application est active.

Vous pouvez contrôler l'application des règles prédéfinies à l'inspection des journaux. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

6. Pour créer une nouvelle règle définie par l'utilisateur, cliquez sur le bouton **Ajouter**.

La fenêtre **Règles d'inspection des journaux** s'ouvre.

7. Dans la section **Général**, saisissez les données suivantes pour la nouvelle règle :

- **Nom de la règle**
- **Source**

Sélectionnez le journal dont les événements sont utilisés pour l'inspection. Vous avez le choix parmi les types de journaux d'événements Windows suivants :

- Application
- Sécurité
- System

Vous pouvez ajouter un nouveau journal personnalisé en saisissant le nom du journal dans le champ **Source**.

8. Dans la section **ID des événements déclenchés**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

- a. Saisissez la valeur numérique de l'identifiant.

- b. Cliquez sur **Ajouter**.

L'identifiant de la règle indiqué est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

- c. Cliquez sur le bouton **OK**.

La règle d'inspection des journaux est ajoutée à la liste générale des règles.

## Administration des règles d'inspection des journaux via la Console de l'application

Cette section explique comment ajouter des règles d'inspection des journaux et les configurer via la Console de l'application.

## Dans cette section

Administration des règles de tâches prédéfinies via la Console de l'application .....	473
Configuration des règles d'inspection des journaux .....	474

## Administration des règles de tâches prédéfinies via la Console de l'application

► *Pour configurer les paramètres de fonctionnement de l'analyse heuristique pour la tâche Inspection des journaux, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Inspection des journaux**.
3. Dans le panneau de détails du nœud **Inspection des journaux**, cliquez sur le lien **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sélectionnez l'onglet **Règles prédéfinies**.
5. Cochez ou décochez la case **Inspecter les journaux selon les règles personnalisées**.

Si cette case est cochée, Kaspersky Security for Windows Server applique l'analyse heuristique pour détecter toute activité anormale sur le serveur protégé.

Si cette case n'est pas cochée, l'analyse heuristique est désactivée, Kaspersky Security for Windows Server utilise les règles prédéfinies ou définies par l'utilisateur pour détecter les activités anormales.

Cette case est cochée par défaut.

Pour que la tâche fonctionne, il faut sélectionner au moins une règle d'inspection des journaux.

6. Sélectionnez les éléments heuristiques que vous souhaitez appliquer à l'inspection des journaux dans la liste des éléments disponibles :
  - Tentative d'attaque brute-force dans le système.
  - Des signes d'abus potentiel du journal des événements Windows ont été détectés.
  - Des actions suspectes émanant d'un nouveau service installé ont été détectées.
  - Une authentification suspecte avec des identifiants explicites a été détectée.
  - Le système affiche les signes d'une éventuelle attaque Kerberos forged PAC (MS14-068).
  - Des actions suspectes contre un groupe Administrateurs privilégié intégré ont été détectées.
  - Une activité suspecte a été détectée lors d'une session de connexion au réseau.
7. Pour configurer les règles sélectionnées, accédez à l'onglet **Etendue**.
8. Dans le groupe **Détection des attaques brute-force**, définissez le nombre de tentatives et l'intervalle d'exécution de celles-ci qui vont servir de critères de déclenchement de l'analyse heuristique.
9. Dans la section **Connexion au réseau**, définissez le début et la fin de l'intervalle de temps pendant lequel



Kaspersky Security for Windows Server considère une tentative d'ouverture de session comme une activité anormale.

10. Sélectionnez l'onglet **Exclusions**.

11. Pour ajouter des utilisateurs considérés comme des utilisateurs de confiance, procédez comme suit :

- a. Cliquez sur le bouton **Parcourir**.
- b. Choisissez l'utilisateur.
- c. Cliquez sur le bouton **OK**.

L'utilisateur indiqué est ajouté à la liste des utilisateurs de confiance.

12. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :

- a. Saisissez l'adresse IP.
- b. Cliquez sur **Ajouter**.

L'adresse IP indiquée est ajoutée à la liste des adresses de confiance.

13. Sous les onglets **Planification** et **Avancé**, configurez les paramètres de planification du lancement de la tâche.

14. Cliquez sur le bouton **OK**.

Les paramètres de la tâche Inspection des journaux sont enregistrés.

## Configuration des règles d'inspection des journaux

Pour ajouter et configurer une nouvelle règle d'inspection des journaux définies par l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Inspection des journaux**.
3. Dans le panneau de détails du nœud **Inspection des journaux**, cliquez sur le lien **Règles d'inspection des journaux**.

La fenêtre **Règles d'inspection des journaux** s'ouvre.

4. Cochez ou décochez la case **Inspecter les journaux selon les règles personnalisées**.

Si cette case est cochée, Kaspersky Security for Windows Server applique les règles définies par l'utilisateur pour l'inspection des journaux conformément aux paramètres de chaque règle. Vous pouvez ajouter, supprimer ou configurer des règles d'inspection des journaux.

Si la case est décochée, vous ne pouvez pas ajouter de règles personnalisées ni en modifier. Kaspersky Security for Windows Server applique les paramètres de règles par défaut.

Cette case est cochée par défaut. Seule la règle de détection de pop-up d'application est active.

Vous pouvez contrôler l'application des règles prédéfinies à la tâche d'inspection des journaux. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

5. Pour créer une règle définie par l'utilisateur, procédez comme suit :

- a. Saisissez le nom de la nouvelle règle.
- b. Cliquez sur **Ajouter**.

La règle créée est ajoutée à la liste générale des règles.

6. Pour configurer n'importe quelle règle, procédez comme suit :

- a. Sélectionnez la règle dans la liste d'un clic gauche de la souris.

Dans la partie droite de la fenêtre, les informations générales relatives à la règle s'affiche sous l'onglet **Description**.

La description de la nouvelle règle est vide.

- b. Sélectionnez l'onglet **Description**.
- c. Dans la section **Général**, modifiez le nom de la règle le cas échéant.
- d. Sélectionnez la **source**.

7. Dans la section **Identificateurs des événements**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

- a. Saisissez la valeur numérique de l'identifiant.
- b. Cliquez sur **Ajouter**.

L'identifiant de la règle indiqué est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

- c. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés des règles d'inspection des journaux sont appliqués.

# Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande et explique la configuration des paramètres de ces tâches ainsi que la configuration des paramètres de la sécurité du serveur protégé.

## Contenu du chapitre

A propos des tâches d'analyse à la demande .....	<a href="#">476</a>
A propos de la zone d'analyse.....	<a href="#">477</a>
Zones d'analyse prédéfinies .....	<a href="#">477</a>
Analyse des fichiers de stockage dans le cloud .....	<a href="#">479</a>
Paramètres de sécurité du nœud sélectionné dans les tâches d'analyse à la demande .....	<a href="#">480</a>
A propos des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	<a href="#">481</a>
A propos de l'analyse des disques amovibles .....	<a href="#">483</a>
Paramètres par défaut de la tâche d'analyse à la demande .....	<a href="#">484</a>
Administration des tâches d'analyse à la demande via le plug-in d'administration.....	<a href="#">486</a>
Administration des tâches d'analyse à la demande via Console de l'application.....	<a href="#">502</a>

## A propos des tâches d'analyse à la demande

Kaspersky Security for Windows Server recherche des virus et autres menaces informatique dans la zone indiquée. Kaspersky Security for Windows Server analyse les fichiers, la mémoire vive du serveur et les objets de démarrage.

Kaspersky Security for Windows Server prévoit les tâches système d'analyse à la demande suivantes :

- La tâche Analyse au démarrage du système d'exploitation est exécutée à chaque démarrage de Kaspersky Security for Windows Server. Kaspersky Security for Windows Server analyse les secteurs et les zones d'amorce des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. Chaque fois que Kaspersky Security for Windows Server exécute la tâche, il crée une copie des secteurs d'amorce non infectés. Si lors du lancement suivant de la tâche, il détecte une menace dans ces secteurs, il les remplace par la copie de sauvegarde.
- La tâche Analyse des zones critiques est exécutée par défaut chaque semaine selon une planification. Kaspersky Security for Windows Server analyse les objets situés dans les zones critiques du système d'exploitation : objets de démarrage, secteurs et zones d'amorce des disques durs et des disques amovibles, mémoire système et mémoire des processus. L'application analyse les fichiers qui se trouvent dans les répertoires système, par exemple dans le dossier %windir%\system32. Kaspersky Security for Windows Server applique les paramètres de sécurité dont les valeurs correspondent au niveau Recommandé (cf. section "A propos des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande" à la page [481](#)). Vous pouvez modifier les paramètres la tâche Analyse des zones critiques.
- La tâche Analyse de la quarantaine est exécutée par défaut selon la programmation après chaque mise à jour des bases de données. Vous ne pouvez pas modifier la zone de la tâche Analyse de la quarantaine.
- La tâche Vérification de l'intégrité de l'application est exécutée tous les jours. Elle permet de vérifier si les modules de Kaspersky Security for Windows Server ont été endommagés ou modifiés. Le dossier

d'installation de l'application est analysé. Les statistiques sur l'exécution des tâches contiennent des informations sur le nombre de modules analysés ou endommagés. Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. Les paramètres de la planification du lancement de la tâche peuvent être modifiés.

Vous pouvez également créer des tâches d'analyse à la demande définie par l'utilisateur, par exemple, une tâche pour l'analyse des dossiers partagés sur le serveur.

Kaspersky Security for Windows Server peut exécuter simultanément plusieurs tâches d'analyse à la demande.

## A propos de la zone d'analyse

Vous pouvez configurer la zone d'analyse pour les tâches Analyse au démarrage du système d'exploitation et Analyse des zones critiques ainsi que pour les tâches d'analyse à la demande définies par l'utilisateur.

Par défaut, les tâches d'analyse à la demande analysent tous les objets du système de fichiers du serveur. Si les exigences en matière de sécurité ne nécessitent pas une analyse de tous les objets du système de fichiers, vous pouvez limiter la zone d'analyse.

Dans la console de l'application, la zone d'analyse se présente sous la forme d'une arborescence ou d'une liste de ressources de fichier de serveur que Kaspersky Security for Windows Server peut contrôler. Par défaut les ressources de fichier réseau du serveur protégé s'affichent sous la forme d'une liste.

► *Pour activer l'affichage des ressources de fichier réseau sous la forme d'une arborescence,*

dans la liste déroulante du coin supérieur gauche de la fenêtre **Configuration de la zone d'analyse**, choisissez l'option **Afficher sous forme d'arborescence**.

Les entrées sont présentées dans une liste ou dans une arborescence des ressources de fichiers du serveur de la manière suivante :

- Nœud repris dans la zone d'analyse.
- Nœud exclu de la zone d'analyse.
- Au moins un des nœuds enfants intégrés à ce nœud est exclu de la zone d'analyse ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur.

L'icône  s'affiche si tous les nœuds enfants ont été sélectionnés, mais pas le nœud parent. Le cas échéant, les modifications du contenu des fichiers et dossiers du nœud parent ne sont pas automatiquement prises en compte lors de la modification de la zone d'analyse du nœud enfant sélectionnée.

Le nom des entrées virtuelles de la zone d'analyse apparaît en lettres bleues.

## Zones d'analyse prédéfinies

L'arborescence ou la liste des ressources fichier de l'ordinateur est affichée dans le panneau de détails de l'entrée de la tâche d'analyse à la demande sélectionnée sous l'onglet **Configuration de la zone d'analyse**.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Security for Windows Server propose les zones d'analyse prédéfinies suivantes :

- **Poste de travail.** Kaspersky Security for Windows Server analyse l'ensemble du serveur.
- **Disques durs locaux.** Kaspersky Security for Windows Server analyse les objets des disques durs d'un serveur. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Disques amovibles.** Kaspersky Security for Windows Server analyse les fichiers sur les périphériques externes tels que les lecteurs de disques compacts ou les lecteurs USB. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Réseau.** Vous pouvez ajouter à la zone 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 dossiers réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte système.

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

- **Mémoire système.** Kaspersky Security for Windows Server analyse les fichiers exécutables et les modules des processus exécutés dans le système d'exploitation au moment de l'analyse.
- **Objets de démarrage.** Kaspersky Security for Windows Server analyse les objets auxquels les clés du registre et les fichiers de configuration font référence, par exemple WIN.INI ou SYSTEM.INI, ainsi que les modules de l'application qui sont lancés automatiquement au démarrage de l'ordinateur.
- **Dossiers partagés.** Vous pouvez ajouter les dossiers partagés du serveur à protéger à la zone d'analyse.
- **Disques virtuels.** Vous pouvez inclure dans la zone d'analyse les disques, les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés sur le serveur, par exemple les disques partagés d'un cluster.

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

Les zones d'analyse prédéfinies s'affichent par défaut dans l'arborescence des ressources de fichier réseau et acceptent l'ajout à la liste des ressources de fichier réseau au moment de sa création dans les paramètres de la zone d'analyse.

Par défaut, les tâches d'analyse à la demande sont exécutées dans les secteurs suivants :

- Tâche Analyse au démarrage du système d'exploitation :
  - **Disques durs locaux ;**

- **Disques amovibles ;**
- **Mémoire système.**
- Analyse des zones critiques :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles ;**
  - **Mémoire système ;**
  - **Objets de démarrage.**
- Autres tâches :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles ;**
  - **Mémoire système ;**
  - **Objets de démarrage ;**
  - **Dossiers partagés.**

## Analyse des fichiers de stockage dans le cloud


### A propos des fichiers cloud


Kaspersky Security for Windows Server peut interagir avec les fichiers sur le cloud Microsoft OneDrive. L'application prend en charge la nouvelle fonction OneDrive Files On-Demand.

Kaspersky Security for Windows Server ne prend pas en charge d'autres stockages cloud

OneDrive Files On-Demand permet d'accéder à tous les fichiers de OneDrive sans avoir à les télécharger tous et à utiliser de l'espace de stockage sur votre appareil. Vous pouvez télécharger des fichiers sur votre disque dur lorsque vous en avez besoin.

Lorsque la fonction OneDrive Files On-Demand est activée, des icônes d'état apparaissent en regard de chaque fichier dans la colonne **Etat** de l'Explorateur de fichiers. Chaque fichier peut prendre un des états suivants :

 Cette icône d'état indique que le fichier est *uniquement disponible en ligne*. Les fichiers uniquement disponibles en ligne ne sont pas stockés sur le disque dur. Vous ne pouvez pas les ouvrir lorsque votre appareil n'est pas connecté à Internet.




 Cette icône d'état indique qu'un fichier est *disponible en local*. Ce cas se produit lorsque vous ouvrez un fichier uniquement disponible en ligne et qu'il se télécharge sur votre appareil. Vous pouvez ouvrir un fichier disponible en local à tout moment même sans accès Internet. Pour gagner de l'espace, vous pouvez redéfinir l'état du fichier sur


 uniquement en ligne.

 Cette icône d'état indique qu'un fichier est *stocké sur le disque dur et toujours disponible*.








### Analyse des fichiers de stockage dans le cloud


Kaspersky Security for Windows Server analyse uniquement les fichiers du cloud lorsqu'ils sont stockés localement

sur un serveur protégé. Ces fichiers OneDrive ont les états  et . Les fichiers  sont ignorés pendant l'analyse car ils ne sont pas physiquement situés sur le serveur protégé.

Kaspersky Security for Windows Server ne télécharge pas automatiquement les  fichiers du Cloud lors de l'analyse, même s'ils figurent dans la zone d'analyse.

Les fichiers du Cloud sont traités par plusieurs tâches de Kaspersky Security for Windows Server dans différents scénarios en fonction du type de tâche :

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone de protection de la tâche Protection des fichiers en temps réel. Le fichier est analysé lorsque l'utilisateur y accède. Si l'utilisateur accède à un fichier , celui-ci est téléchargé, devient disponible en local et a désormais l'état . Cela permet à la tâche Protection des fichiers en temps réel de traiter le fichier :
- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone d'analyse de la tâche Analyse à la demande. La tâche analyse les fichiers avec les états  et . Si des fichiers  sont trouvés dans la zone, ils seront ignorés pendant l'analyse et un événement d'information sera enregistré dans le journal d'exécution de la tâche. Il indiquera que le fichier analysé n'est qu'une marque de réservation pour un fichier cloud et n'existe pas sur un disque local.
- Génération des règles du Contrôle des applications et utilisation : vous pouvez créer des règles d'autorisation et d'interdiction pour les fichiers  et  à l'aide de la tâche Génération des règles du Contrôle du lancement des applications. La tâche Contrôle du lancement des applications applique le principe Interdire par défaut et des règles créées pour traiter et interdire les fichiers cloud.

La tâche Contrôle du lancement des applications bloque le lancement de tous les fichiers dans le Cloud, peu importe leur état. Les fichiers  ne sont pas inclus dans la zone de génération de règles par l'application car ils ne sont pas physiquement stockés sur un disque dur. Aucune règle d'autorisation ne peut être créée pour ces fichiers. Par conséquent, ils sont soumis au principe Interdire par défaut.

Lorsqu'une menace est détectée sur un fichier cloud OnDrive, l'application exécute l'action spécifiée dans les paramètres de la tâche effectuant l'analyse. Ainsi, le fichier peut être supprimé, désinfecté, placé en quarantaine ou sauvegardé.

Les modifications apportées aux fichiers locaux sont synchronisées avec les copies stockées sur OneDrive conformément aux principes exposés dans la documentation Microsoft OneDrive correspondante.

## Paramètres de sécurité du nœud sélectionné dans les tâches d'analyse à la demande

Dans la tâche d'analyse à la demande sélectionnée, vous pouvez modifier les valeurs des paramètres de sécurité par défaut de la même manière pour toute la zone de protection ou d'analyse ou avec des variations pour différentes

entrées ou éléments dans l'arborescence ou la liste des ressources de fichiers du serveur.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

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

- Sélectionner un des trois niveaux de sécurité prédéfinis (**Recommandé**, **Performance maximale** ou **Protection maximale**) ;
- Modifier manuellement les paramètres de sécurité pour les entrées sélectionnées de l'arborescence ou de la liste des ressources fichier du serveur (le niveau de sécurité prend alors la valeur **Personnalisé**).

Vous pouvez enregistrer la sélection de paramètres du nœud dans un modèle afin de l'appliquer à d'autres nœuds.

## A propos des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Les paramètres de sécurité **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique** et **Vérifier la signature Microsoft des fichiers** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si vous modifiez la valeur des paramètres **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique** ou **Vérifier la signature Microsoft des fichiers**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

Vous pouvez appliquer un des trois niveaux de sécurité prédéfinis pour un nœud sélectionné dans l'arborescence des ressources de fichier du serveur : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

### Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si des mesures de sécurité du serveur complémentaires ont été adoptées dans votre réseau, telles que des pare-feu ou des stratégies de sécurité, en plus de Kaspersky Security for Windows Server.

### Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

### Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité informatique élevé.



Tableau 67. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondants

Options	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
<b>Analyser les objets</b>	En fonction du format	Tous les objets	Tous les objets
<b>Analyser uniquement les nouveaux fichiers et les fichiers modifiés</b>	Activée	Désactivée	Désactivée
<b>Actions à exécuter sur les objets infectés et autres</b>	Désinfecter. Supprimer si la désinfection est impossible	Exécuter l'action recommandée (Désinfecter. Supprimer si la désinfection est impossible)	Désinfecter. Supprimer si la désinfection est impossible
<b>Actions à exécuter sur les objets probablement infectés</b>	Quarantaine	Exécuter l'action recommandée (quarantaine)	Quarantaine
<b>Exclure les fichiers</b>	non	non	non
<b>Ne pas détecter</b>	non	non	non
<b>Arrêter si l'analyse dure plus de (s.)</b>	60 s	non	non
<b>Ne pas analyser les objets composés de plus de (Mo)</b>	8 Mo	non	non
<b>Analyser les flux NTFS alternatifs</b>	Oui	Oui	Oui
<b>Analyser les secteurs d'amorçage et la partition MBR</b>	Oui	Oui	Oui
<b>Analyse des objets composés</b>	<ul style="list-style-type: none"> <li>• Archives SFX*</li> <li>• Objets compactés*</li> <li>• Objets OLE intégrés*</li> </ul> <p>* uniquement les objets nouveaux et modifiés</p>	<ul style="list-style-type: none"> <li>• Archives*</li> <li>• Archives SFX*</li> <li>• Objets compactés*</li> <li>• Objets OLE intégrés*</li> </ul> <p>* Tous les objets</p>	<ul style="list-style-type: none"> <li>• Archives*</li> <li>• Archives SFX*</li> <li>• Bases de données d'emails*</li> <li>• Message de texte plat*</li> <li>• Objets compactés*</li> <li>• Objets OLE intégrés*</li> </ul> <p>* Tous les objets</p>

## A propos de l'analyse des disques amovibles

Vous pouvez configurer l'analyse des disques amovibles connectés via USB au serveur protégé.

Kaspersky Security for Windows Server analyse le disque amovible à l'aide de la tâche Analyse à la demande. L'application crée automatiquement une tâche Analyse à la demande lors de la connexion du disque amovible et supprime cette tâche à la fin de l'analyse. La tâche créée est exécutée selon le niveau de sécurité prédéfini pour l'analyse des disques amovibles. Vous ne pouvez pas configurer les paramètres de la tâche temporaire Analyse à la demande.

Si vous avez installé Kaspersky Security for Windows Server sans bases antivirus, l'analyse des disques amovibles n'est pas disponible.

Kaspersky Security for Windows Server lance l'analyse des disques amovibles connectés via USB lorsque ces derniers sont enregistrés dans le système d'exploitation en tant que périphérique de stockage de masse (USB Mass Storage Device). L'application n'analyse pas le disque amovible si la tâche Contrôle des périphériques a bloqué la connexion de ce dernier. L'application ne lance pas l'analyse des périphériques mobiles MTP.

Kaspersky Security for Windows Server autorise l'accès aux disques amovibles durant l'analyse.

Les résultats de l'analyse de chaque disque amovible peuvent être consultés dans le journal d'exécution de la tâche Analyse à la demande créée lors de la connexion de ce disque.

Vous pouvez modifier les valeurs des paramètres du composant Analyse des disques amovibles (cf. tableau ci-dessous).

Tableau 68. Paramètres d'analyse des disques amovibles

Paramètre	Valeur par défaut	Description
<b>Analyser les disques amovibles à la connexion via USB</b>	Case décochée	Vous pouvez activer ou désactiver l'analyse des disques amovibles lors de leur connexion au serveur protégé via USB.
<b>Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)</b>	1024 MB	Vous pouvez réduire la plage de déclenchement du composant en indiquant le volume de données maximum sur le disque amovible. Kaspersky Security for Windows Server ne lance pas l'analyse du disque amovible si le volume des données qu'il contient est supérieur à la valeur indiquée.

<b>Analyser avec le niveau de sécurité</b>	Protection maximale	<p>Vous pouvez configurer les paramètres des tâches d'analyse à la demande créées en choisissant un de trois niveaux de sécurité suivants :</p> <ul style="list-style-type: none"> <li>• <b>Protection maximale</b></li> <li>• <b>Recommandé</b></li> <li>• <b>Performance maximale</b></li> </ul> <p>L'algorithme des actions à effectuer lors de la détection d'objets infectés, probablement infectés et autres, ainsi que d'autres paramètres d'analyse pour chaque niveau de sécurité correspondent aux niveaux de sécurité préétablis dans les tâches d'analyse à la demande.</p>
--	---------------------	---

## Paramètres par défaut de la tâche d'analyse à la demande

Par défaut, les tâches d'analyse à la demande possèdent les paramètres décrits dans le tableau ci-dessous. Vous pouvez configurer les tâches d'analyse à la demande système et définies par l'utilisateur.

Tableau 69. Paramètres par défaut de la tâche d'analyse à la demande

Paramètre	Valeur	Description
Zone d'analyse	<p>S'applique aux tâches système et définies par l'utilisateur :</p> <ul style="list-style-type: none"> <li>• <b>Analyse au démarrage du système d'exploitation</b> : tout le serveur, à l'exception des dossiers partagés et des objets de démarrage ;</li> <li>• <b>Analyse des zones critiques</b> : tout le serveur, à l'exception des dossiers partagés et de certains fichiers du système d'exploitation ;</li> <li>• <b>Tâches d'Analyse à la demande</b> définie par l'utilisateur : tout le serveur.</li> </ul>	<p>Vous pouvez modifier la zone d'analyse. Il est impossible de configurer la zone d'analyse pour les tâches système <b>Analyse de la quarantaine</b> et <b>Vérification de l'intégrité de l'application</b>.</p>
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; correspondent au niveau de sécurité <b>Recommandé</b> .	<p>Pour les entrées sélectionnées dans l'arborescence ou dans la liste des ressources de fichiers de l'ordinateur, vous pouvez exécuter les actions suivantes :</p> <ul style="list-style-type: none"> <li>• Sélectionner un autre niveau de sécurité prédéfini ;</li> <li>• Modifier manuellement les paramètres de sécurité.</li> </ul> <p>Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à n'importe quel autre nœud.</p>

Paramètre	Valeur	Description
<b>Utiliser l'analyse heuristique</b>	Les tâches Analyse des zones critiques et Analyse au démarrage du système d'exploitation, aussi que les tâches d'analyse définies par l'utilisateur, sont exécutées selon la valeur <b>Moyenne</b> . La tâche Analyse de la quarantaine est réalisée selon la valeur <b>Minutieuse</b> .	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse. Vous ne pouvez pas configurer le niveau d'analyse pour la tâche Analyse de la quarantaine. L'application de l'analyse heuristique n'est pas prévue dans la tâche Vérification de l'intégrité de l'application.
<b>Appliquer la zone de confiance</b>	Appliqué (pas appliquée pour la tâche Analyse de la quarantaine)	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.
<b>Utiliser KSN pour l'analyse</b>	Appliquée.	Vous pouvez améliorer l'efficacité de la protection du serveur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Paramètres du lancement de la tâche avec autorisations	La tâche est lancée sous les autorisations du compte système.	Vous pouvez modifier les paramètres de lancement sous les autorisations d'un compte pour tous les tâches d'analyse à la demande système ou définies par l'utilisateur, sauf pour les tâches Analyse de la quarantaine et Vérification de l'intégrité de l'application.
<b>Exécuter la tâche en arrière-plan (priorité basse)</b>	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.
Planification du lancement de la tâche	S'applique aux tâches système : <ul style="list-style-type: none"> <li>Analyse au démarrage du système d'exploitation : <b>Au lancement de l'application</b> ;</li> <li>Analyse des zones critiques : <b>Toutes les semaines</b> ;</li> <li>Analyse de la quarantaine : <b>A la mise à jour des bases de l'application</b> ;</li> <li>Vérification de l'intégrité de l'application - <b>Tous les jours</b></li> </ul> Pas appliqué dans les tâches définies par l'utilisateur recréées.	Vous pouvez configurer les paramètres de lancement de la tâche planifiée.

Paramètre	Valeur	Description
Enregistrement de l'exécution de l'analyse et de la mise à jour de l'état de la protection du serveur	L'état de la protection du serveur est actualisé chaque semaine après l'exécution de la tâche Analyse des zones critiques.	<p>Vous pouvez configurer les paramètres d'enregistrement de l'exécution de l'analyse rapide d'une des manières suivantes :</p> <ul style="list-style-type: none"> <li>• En modifiant les paramètres de la planification du lancement de la tâche Analyse des zones critiques.</li> <li>• En modifiant la zone d'analyse de la tâche Analyse des zones critiques.</li> <li>• En créant des tâches d'analyse à la demande définies par l'utilisateur.</li> </ul>

## Administration des tâches d'analyse à la demande via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des serveurs du réseau.

### Dans cette section

Navigation .....	<a href="#">486</a>
Création d'une tâche d'analyse à la demande.....	<a href="#">488</a>
Configuration de la zone d'analyse de la tâche.....	<a href="#">493</a>
Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	<a href="#">494</a>
Configuration manuelle des paramètres de sécurité .....	<a href="#">495</a>
Configuration de l'analyse des disques amovibles .....	<a href="#">502</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Ouverture de l'assistant de tâche d'analyse à la demande .....	<a href="#">486</a>
Accès aux propriétés de la tâche d'analyse à la demande .....	<a href="#">488</a>

## Ouverture de l'assistant de tâche d'analyse à la demande

► *Pour commencer à créer une tâche d'analyse à la demande définie par l'utilisateur, procédez comme*

*suit :*

1. Pour créer une tâche locale :
  - a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
  - b. Sélectionnez le groupe d'administration auquel appartient le serveur.
  - c. Dans le panneau de détails, sous l'onglet **Périphériques**, ouvrez le menu contextuel du serveur protégé.
  - d. Sélectionnez l'option de menu **Propriétés**.
  - e. Dans la section **Tâches** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

La fenêtre **Assistant de nouvelle tâche** s'ouvre.

2. Pour créer une tâche de groupe :
  - a. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
  - b. Sélectionnez le groupe d'administration pour lequel vous souhaitez créer une tâche.
  - c. Ouvrez l'onglet **Tâches**.
  - d. Cliquez sur le bouton **Créer une tâche**.

La fenêtre **Assistant de nouvelle tâche** s'ouvre.

3. Pour créer une tâche pour un ensemble de serveurs défini par l'utilisateur :
  - a. Dans le nœud **Sélections de périphériques** de l'arborescence de la Console d'administration de Kaspersky Security Center, cliquez sur le bouton **Exécuter une sélection** pour sélectionner un périphérique.
  - b. Ouvrez l'onglet **Résultats de la sélection pour "nom de la sélection"**.
  - c. Dans la liste déroulante **Réaliser une sélection**, sélectionnez l'option **Créer une tâche pour un résultat de sélection**.

La fenêtre **Assistant de nouvelle tâche** s'ouvre.

4. Sélectionnez la tâche **Analyse à la demande** dans la liste des tâches disponibles pour Kaspersky Security for Windows Server.
5. Cliquez sur **Suivant**.

La fenêtre **Configuration** s'ouvre.

Configurez les paramètres de la tâche en fonction des besoins.

► *Pour configurer une tâche existante d'analyse à la demande :*

Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

La fenêtre **Propriétés : Analyse à la demande** s'ouvre.

## Accès aux propriétés de la tâche d'analyse à la demande

- Pour accéder aux propriétés de l'application pour la tâche Analyse à la demande pour un serveur unique :
1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
  2. Sélectionnez le groupe d'administration auquel appartient le serveur protégé.
  3. Sélectionnez l'onglet **Périphériques**.
  4. Double-cliquez sur le nom du serveur pour lequel vous souhaitez configurer une zone d'analyse.  
La fenêtre **Propriétés : "nom du serveur"** s'ouvre.
  5. Sélectionnez la section **Tâches**.
  6. Dans la liste des tâches créées pour le périphérique, sélectionnez la tâche Analyse à la demande que vous avez créée.
  7. Cliquez sur le bouton **Propriétés**.  
La fenêtre **Propriétés : Analyse à la demande** s'ouvre.
- Configurez les paramètres de la tâche en fonction des besoins.

## Création d'une tâche d'analyse à la demande

- Pour créer une tâche d'analyse à la demande définie par l'utilisateur, procédez comme suit :
1. Ouvrez la fenêtre **Configuration** (cf. section "**Ouverture de l'assistant de tâche d'analyse à la demande**" à la page [486](#)) dans l'**assistant Nouvelle tâche**.
  2. Sélectionnez le **Mode de création de la tâche** requis.
  3. Cliquez sur **Suivant**.
  4. Dans la fenêtre **Zone d'analyse**, définissez la zone d'analyse.

La zone d'analyse reprend par défaut les secteurs critiques du serveur. Les zones d'analyse sont accompagnées de l'icône  dans le tableau. Les zones d'analyse exclues sont accompagnées de l'icône  dans le tableau.

Vous pouvez modifier la zone d'analyse, y inclure des zones distinctes prédéfinies, des disques, des dossiers, des objets de réseaux et des fichiers et définir les paramètres particuliers de la protection pour chaque zone ajoutée.

- Pour exclure de l'analyse toutes les zones d'analyse critiques, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.
- Pour inclure une zone d'analyse, un disque, un dossier, un objet réseau ou un fichier prédéfini dans la zone d'analyse :
  - a. Cliquez avec le bouton droit de la souris dans le tableau **Zone d'analyse** et choisissez l'option **Ajouter une zone** ou cliquez sur le bouton **Ajouter**.
  - b. Dans la fenêtre **Ajouter des objets à la zone d'analyse**, sélectionnez la zone prédéfinie dans la

liste **Zone prédéfinie**, désignez le disque de l'ordinateur, le dossier, l'objet réseau ou le fichier sur le serveur ou sur un autre ordinateur du réseau, puis cliquez sur le bouton **OK**.

- Pour exclure des sous-dossiers ou des fichiers de l'analyse, sélectionnez le dossier (le disque) ajouté dans la fenêtre **Zone d'analyse** de l'assistant :
  - a. Ouvrez le menu contextuel et sélectionnez l'option **Configurer**.
  - b. Cliquez sur le bouton **Configuration** afin d'ouvrir la fenêtre **Niveau de sécurité**.
  - c. Sous l'onglet **Général** de la fenêtre **Paramètres de l'analyse à la demande**, décochez les cases **Sous-dossiers** et **Sous-fichiers**.
- Pour modifier les paramètres de sécurité de la zone d'analyse :
  - a. Ouvrez le menu contextuel de la zone dont vous souhaitez modifier les paramètres et choisissez l'option **Configurer**.
  - b. Dans la fenêtre **Paramètres de l'analyse à la demande**, sélectionnez un des niveaux de sécurité prédéfinis ou cliquez sur le bouton **Configuration** afin de configurer manuellement les paramètres de sécurité.

Les paramètres de sécurité sont configurés de la même manière que la tâche Protection des fichiers en temps réel (cf. section "Configuration manuelle des paramètres de sécurité" à la page [264](#)).

- Pour ignorer les objets joints dans la zone d'analyse ajoutée :
  - a. Ouvrez le menu contextuel du tableau **Zone d'analyse** et sélectionnez **Ajouter une exclusion** une exclusion.
  - b. Désignez les objets à exclure : sélectionnez une zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque de l'ordinateur, le dossier, l'objet réseau ou le dossier sur le serveur ou tout autre ordinateur du réseau.
  - c. Cliquez sur le bouton **OK**.
- 5. Dans la section **Options**, configurez l'analyse heuristique et l'intégration aux autres modules :
  - Configurez l'utilisation de l'analyse heuristique (cf. section "Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application" à la page [260](#))
  - Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure de la zone d'analyse les objets ajoutés à la Zone de confiance.

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

- Cochez la case **Utiliser KSN pour l'analyse** si vous souhaitez utiliser les services cloud de Kaspersky Security Network pour la tâche.

La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network



(KSN) dans la tâche.

Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

Si la case est décochée, la tâche d'analyse à la demande n'utilise pas les services du KSN.

Cette case est cochée par défaut.

- Pour attribuer la priorité de base *faible* (Low) au processus de travail dans lequel la tâche va être exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Options**.

La case modifie la priorité de la tâche.

Si la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et le système de fichiers du serveur par les autres tâches de Kaspersky Security for Windows Server ou les autres applications. Par conséquent la vitesse d'exécution de la tâche diminue quand la charge augmente et inversement.

Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security for Windows Server et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

Cette case est décochée par défaut.

Par défaut, les processus dans lesquels les tâches de Kaspersky Security for Windows Server sont exécutées ont la priorité *Moyenne* (Normale).

- Pour utiliser la tâche créée en tant que tâche d'analyse rapide, cochez la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** dans la fenêtre **Options**.

La case modifie la priorité de la tâche : active ou désactive l'enregistrement des événements dans le journal *Analyse des zones critiques* et l'actualisation de l'état de la protection du serveur. Kaspersky Security Center évalue la sécurité du ou des serveurs sur la base des résultats des performances des tâches portant l'état *Analyse des zones critiques*. La case n'est pas accessible dans les propriétés des tâches locales du système ou définies par l'utilisateur dans Kaspersky Security for Windows Server. Vous pouvez modifier ce paramètre uniquement du côté de Kaspersky Security Center.

Si la case est cochée, le Serveur d'administration consigne l'événement Analyse des zones critiques réalisée et actualise l'état de la protection du serveur sur la base des résultats de l'exécution de la tâche. La priorité de la tâche d'analyse est élevée.

Si la case est décochée, la tâche d'analyse est exécutée selon une priorité faible.

La case est cochée par défaut pour les tâches d'analyse à la demande définie par l'utilisateur.

6. Cliquez sur **Suivant**.
7. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.
8. Cliquez sur **Suivant**.
9. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.

10. Cliquez sur **Suivant**.
11. Définissez un nom de tâche.
12. Cliquez sur **Suivant**.

Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants :  
" \* < > & \ : |

La fenêtre **Fin de la création de la tâche** s'ouvre.

13. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.
14. Cliquez sur **Terminer** pour terminer la création de la tâche.

Une tâche Analyse à la demande est créée pour un serveur ou un groupe de serveurs sélectionnés.

## Dans cette section

Attribution de l'état "Analyse des zones critiques" à la tâche d'analyse à la demande .....	<a href="#">491</a>
Exécution en arrière-plan de la tâche d'analyse à la demande .....	<a href="#">492</a>
Enregistrement de l'exécution de l'analyse rapide .....	<a href="#">493</a>

## Attribution de l'état "Analyse des zones critiques" à la tâche d'analyse à la demande

Kaspersky Security Center attribue par défaut l'état *Avertissement* au serveur si la tâche Analyse des zones critiques est exécutée moins souvent que ne l'indique le paramètre du seuil de génération d'événement de Kaspersky Security for Windows Server **Analyse des zones critiques non réalisée depuis longtemps**.

► *Pour configurer l'analyse de tous les serveurs appartenant à un groupe d'administration, procédez comme suit :*

1. Créez une tâche de groupe d'Analyse à la demande (cf. section "Création d'une tâche d'analyse à la demande" à la page [488](#)).
2. Dans la fenêtre **Options** de l'Assistant de création de tâches, cochez la case **Considérer l'exécution de la tâche comme une analyse des zones critiques**. Les paramètres que vous aurez définis (zone d'analyse et paramètres de sécurité) seront identiques pour tous les serveurs du groupe. Programmez l'exécution de la tâche.

Vous pouvez cocher la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** lors de la création d'une tâche d'analyse à la demande pour un groupe de serveurs ou plus tard dans la fenêtre **Propriétés : <nom de la tâche>** (cf. section "Accès aux propriétés de la tâche d'analyse à la demande" à la page [488](#)).

3. A l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez le lancement planifié des tâches d'analyse à la demande prédéfinies (cf. section "Configuration du lancement planifié des tâches locales du système" à la page [104](#)).

Dès ce moment, le Serveur d'administration de Kaspersky Security Center évalue la protection du serveur protégé et vous en informe sur la base de la dernière exécution de la tâche portant l'état de l'Analyse des zones critiques et non sur la base des résultats de la tâche système *Analyse des zones critiques*.

Vous pouvez attribuer l'état *Tâche d'analyse rapide* à des tâches de groupe d'analyse à la demande ou à des tâches pour des sélections d'ordinateurs.

La console de l'application permet de voir si la tâche d'analyse à la demande est une tâche d'analyse rapide.

Dans la console de l'application, la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** apparaît dans la propriété des tâches mais elle ne peut pas être modifiée.

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

Par défaut, les processus dans lesquels les tâches de Kaspersky Security for Windows Server sont exécutées ont la priorité de base *Moyenne* (Normal).

Vous pouvez attribuer la priorité de base *faible* (Low) au processus dans lequel la tâche d'analyse à la demande va être 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 pour les tâches d'analyse à la demande en arrière-plan.

► *Pour modifier la priorité d'une tâche d'analyse à la demande existante, procédez comme suit !*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "Ouverture de l'assistant de tâche d'analyse à la demande" à la page [486](#)).
2. Cochez ou décochez la case **Exécuter la tâche en arrière-plan**.

La case modifie la priorité de la tâche.

Si la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et le système de fichiers du serveur par les autres tâches de Kaspersky Security for Windows Server ou les autres applications. Par conséquent la vitesse d'exécution de la tâche diminue quand la charge augmente et inversement.

Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security for Windows Server et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

Cette case est décochée par défaut.

3. Cliquez sur le bouton **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

## Enregistrement de l'exécution de l'analyse rapide

Par défaut, l'état de la protection du serveur apparaît dans le panneau de détails du nœud **Kaspersky Security** et il est actualisé chaque semaine après la fin de la tâche Analyse des zones critiques.

L'heure de l'actualisation de l'état de la protection du serveur est liée à la planification de la tâche d'analyse à la demande où la case **Considérer l'exécution de la tâche comme une analyse des zones critiques** a été cochée dans les paramètres. Par défaut, la case est cochée uniquement pour la tâche Analyse des zones critiques et ne peut être modifiée pour cette tâche.

Vous pouvez sélectionner la tâche d'analyse à la demande associée à l'état de la protection du serveur uniquement au départ de Kaspersky Security Center.

## Configuration de la zone d'analyse de la tâche

Si vous modifiez la zone d'analyse dans les tâches Analyse au démarrage du système d'exploitation et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la restauration de Kaspersky Security for Windows Server (**Démarrer > Programmes > Kaspersky Security for Windows Server > Modification ou suppression de Kaspersky Security for Windows Server**). Dans l'assistant d'installation, sélectionnez l'option **Réparation des composants installés**, cliquez sur **Suivant**, puis cochez la case **Rétablir les paramètres recommandés de l'application**.

► *Pour configurer une zone d'analyse pour une tâche d'analyse à la demande existante :*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "Accès aux propriétés de la tâche d'analyse à la demande" à la page [488](#)).
2. Ouvrez l'onglet **Zone d'analyse**.
3. Pour inclure des éléments dans la zone d'analyse, procédez comme suit :
  - a. Ouvrez le menu contextuel dans l'espace vide de la liste de zone d'analyse.
  - b. Sélectionnez l'option **Ajouter une zone** dans le menu contextuel.
  - c. Dans la fenêtre **Ajouter des objets à la zone d'analyse** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter à la zone d'analyse :
    - **Zone prédéfinie**, si vous voulez ajouter une des zones prédéfinies sur un serveur protégé. Puis, dans la liste déroulante, choisissez la zone d'analyse nécessaire.
    - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone d'analyse un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone requise en cliquant sur le bouton **Parcourir**.
    - **Fichier**, si vous voulez insérer dans la zone d'analyse uniquement un fichier distinct sur le disque. Puis choisissez la zone requise en cliquant sur le bouton **Parcourir**.

Vous ne pouvez pas ajouter un objet à la zone d'analyse s'il est déjà ajouté en tant qu'exclusion de la zone de protection.

4. Pour exclure certaines entrées de la zone d'analyse, décochez les cases en regard des noms de ces

entrées ou réalisez les opérations suivantes :

- a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.
- b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.
- c. Dans la fenêtre **Ajouter une exclusion**, choisissez le type de l'objet que vous voulez ajouter à titre d'exclusion de la zone d'analyse, de la même manière que l'ajout d'un objet à la zone d'analyse.
5. Pour modifier la zone d'analyse ou une exclusion ajoutée, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Modifier la zone**.
6. Pour masquer la zone d'analyse ou une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Supprimer une zone**.

La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.

7. Cliquez sur le bouton **OK**.

La fenêtre Configuration de la zone d'analyse se ferme. Les paramètres de la tâche définis seront enregistrés.

## Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour un élément sélectionné dans la liste des ressources de fichier réseau du serveur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé**, et **Protection maximale**.

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "**Accès aux propriétés de la tâche d'analyse à la demande**" à la page [488](#)).
2. Ouvrez l'onglet **Zone d'analyse**.
3. Dans la liste du serveur, sélectionnez un élément repris dans la zone d'analyse afin de définir le niveau de sécurité prédéfini.
4. Cliquez sur le bouton **Configurer**.

La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

5. Sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité que vous souhaitez appliquer.  
La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau de sécurité que vous avez sélectionné.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : Analyse à la demande**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

## Configuration manuelle des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé** (cf. section "Niveaux de sécurité prédéfinis" à la page [251](#)).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers du serveur.

► *Pour configurer manuellement les paramètres de sécurité :*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "Accès aux propriétés de la tâche d'analyse à la demande" à la page [488](#)).
2. Ouvrez l'onglet **Zone d'analyse**.
3. Sélectionnez les éléments dans la liste de zone d'analyse pour lesquels vous souhaitez configurer les paramètres de sécurité.

Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité (cf. section "A propos des modèles de paramètres de sécurité" à la page [164](#)) à un nœud ou un élément sélectionné dans la zone d'analyse.

4. Cliquez sur le bouton **Configurer**.  
La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.
5. Configurez les paramètres de sécurité requis pour le nœud ou l'élément sélectionné en fonction de vos exigences :
  - Paramètres **Général** (cf. section "Configuration des règles prédéfinies d'une tâche" à la page [496](#))
  - **Actions** (cf. section "**Configuration des actions**" à la page [498](#))
  - **Optimisation** (cf. section "**Configuration de l'optimisation**" à la page [500](#))
6. Cliquez sur **OK** dans la fenêtre **Paramètres de l'analyse à la demande**.
7. Dans la fenêtre **Zone d'analyse**, cliquez sur **OK**.

Les paramètres de la nouvelle zone d'analyse sont enregistrés.

### Dans cette section

Configuration des paramètres de tâche généraux .....	<a href="#">496</a>
Configuration des actions .....	<a href="#">498</a>
Configuration de l'optimisation.....	<a href="#">500</a>

## Configuration des paramètres de tâche généraux

► Pour configurer les paramètres généraux de la tâche *Analyse à la demande*, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "**Accès aux propriétés de la tâche d'analyse à la demande**" à la page [488](#)).

2. Ouvrez l'onglet **Zone d'analyse**.

3. Cliquez sur le bouton **Configurer**.

La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

4. Cliquez sur le bouton **Configuration**.

5. Dans la section **Analyser les objets** de l'onglet **Général**, indiquez les types d'objets que vous souhaitez inclure dans la zone d'analyse :

- **Objets à analyser**

- **Tous les objets**

Kaspersky Security for Windows Server analyse tous les objets.

- **Objets analysés en fonction du format**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.

Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**

Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

- **Sous-dossiers**

- **Sous-fichiers**

- **Analyser les secteurs d'amorçage et la partition MBR**

Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

Si la case est cochée, Kaspersky Security for Windows Server analyse les secteurs et les zones d'amorce sur les disques durs et les disques amovibles du serveur.

Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**

Analyse des flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

Si la case est cochée, l'application analyse un objet probablement infecté et tous les flux

NTFS associés à cet objet.

Si la case est décochée, l'application analyse uniquement l'objet qui a été détecté et considéré comme probablement infecté.

Cette case est cochée par défaut.

6. Dans le section **Optimisation**, cochez ou décochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security for Windows Server a identifiés comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

Si la case est cochée, Kaspersky Security for Windows Server analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

Si la case est décochée, vous pouvez décider si vous souhaitez analyser et protéger uniquement les nouveaux fichiers ou tous les fichiers, quel que soit leur état de modification.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Protection maximale** ou **Recommandé**, la case est décochée.

Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.

7. Dans la section **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

- **Toutes les/ Les nouvelles archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Toutes les /Les nouvelles archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données d'emails**

Analyse des fichiers des bases de données de messagerie de Microsoft Outlook et Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers des



bases de données de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers des bases de données de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Tous les / Les nouveaux messages de texte brut**

Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers aux formats de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers aux formats de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

8. Cliquez sur le bouton **OK**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration des actions

► *Pour configurer les actions sur les objets infectés et les autres objets détectés lors de la tâche Analyse à la demande, procédez comme suit :*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "**Accès aux propriétés de la tâche d'analyse à la demande**" à la page [488](#)).
2. Ouvrez l'onglet **Zone d'analyse**.
3. Cliquez sur le bouton **Configurer**.

La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

4. Cliquez sur le bouton **Configuration**.
5. Sélectionnez l'onglet **Actions**.
6. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Désinfecter.**
- **Désinfecter. Supprimer si la désinfection est impossible.**
- **Supprimer.**
- **Exécuter l'action recommandée.**

7. Sélectionnez l'action à exécuter sur les objets probablement infectés :

- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Quarantaine.**
- **Supprimer.**
- **Exécuter l'action recommandée.**

8. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

- a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

Si la case est cochée, vous pouvez indépendamment définir une action principale et secondaire pour chaque type d'objet détecté en cliquant sur le bouton **Configuration** en regard de la case. De plus, Kaspersky Security for Windows Server ne permet pas d'ouvrir ou d'exécuter un objet infecté, quel que soit votre choix.

Si la case est décochée, Kaspersky Security for Windows Server exécute les actions sélectionnées dans les sections **Actions à exécuter sur les objets infectés et autres** et **Actions à exécuter sur les objets probablement infectés** des types d'objets nommés,

respectivement.

Cette case est décochée par défaut.

- b. Cliquez sur le bouton **Configuration**.
  - c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (si la première échoue) pour chaque type d'objet détecté.
  - d. Cliquez sur le bouton **OK**.
9. Choisissez l'action à exécuter sur les objets composés qui ne peuvent être désinfectés : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**

La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.

10. Cliquez sur le bouton **OK**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration de l'optimisation

► *Pour configurer la performance de la tâche Analyse à la demande :*

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande** (cf. section "**Accès aux propriétés de la tâche d'analyse à la demande**" à la page [488](#)).

2. Ouvrez l'onglet **Zone d'analyse**.

3. Cliquez sur le bouton **Configurer**.

La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

4. Cliquez sur le bouton **Configuration**.

5. Sélectionnez l'onglet **Optimisation**.

6. Dans la section **Exclusions** :

- Cochez ou décochez la case **Exclure les fichiers**.

Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse tous les objets.

Cette case est décochée par défaut.

- Cochez ou décochez la case **Ne pas détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus

<https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

## 7. Dans la section **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets composés de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Si la case est cochée, Kaspersky Security for Windows Server ignore pour la recherche de virus les objets composés dont la taille est supérieure à la valeur indiquée.

Si la case est décochée, Kaspersky Security for Windows Server analyse les objets composés sans tenir compte de la taille.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Utiliser la technologie iSwift**

iSwift compare l'identifiant NTFS du fichier, identifiant stocké dans une base de données, avec un identifiant en cours. L'analyse est effectuée uniquement pour les fichiers dont les identifiant ont changé (nouveaux fichiers et fichiers modifiés depuis la dernière analyse des objets système NTFS).

Si la case est cochée, Kaspersky Security for Windows Server analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse des objets système NTFS.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers du système NTFS en ignorant la date de création ou de modification sauf pour les fichiers des dossiers réseau.

Cette case est cochée par défaut.

- **Utiliser la technologie iChecker**

iChecker calcule et enregistre les sommes de contrôle des fichiers analysés. Si un objet est modifié, la somme de contrôle change. L'application compare toutes les sommes de contrôle pendant la tâche d'analyse et analyse uniquement les fichiers nouveaux et

modifiés depuis la dernière analyse de fichiers.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers nouveaux et modifiés.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers en ignorant leur date de création ou de modification.

Cette case est cochée par défaut.

8. Cliquez sur le bouton **OK**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration de l'analyse des disques amovibles

► Pour configurer l'analyse des disques amovibles lorsqu'ils sont connectés au serveur protégé, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.

Dans la fenêtre **Propriétés** : **<nom de la stratégie>** qui s'ouvre, sélectionnez la section **Complémentaire**.

5. Cliquez sur le bouton **Configuration** dans la sous-section **Analyse des disques amovibles**.

La fenêtre **Analyse des disques amovibles** s'ouvre.

6. Dans la section **Analyse à la connexion**, procédez comme suit :
  - Cochez la case **Analyser les disques amovibles à la connexion via USB** si vous souhaitez que Kaspersky Security for Windows Server lance automatiquement l'analyse des disques amovibles à la connexion.
  - Le cas échéant, cochez la case **Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
  - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.

7. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés et appliqués.

## Administration des tâches d'analyse à la demande via Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un serveur local.

## Dans cette section

Navigation .....	<a href="#">503</a>
Création et configuration d'une tâche d'analyse à la demande .....	<a href="#">503</a>
Zone d'analyse dans les tâches d'analyse à la demande .....	<a href="#">506</a>
Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande .....	<a href="#">510</a>
Configuration manuelle des paramètres de sécurité .....	<a href="#">510</a>
Analyse des disques amovibles.....	<a href="#">517</a>
Statistiques des tâches d'analyse à la demande.....	<a href="#">518</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres de la tâche d'analyse à la demande .....	<a href="#">503</a>
---	---------------------

## Accès aux paramètres de la tâche d'analyse à la demande

► *Pour ouvrir les paramètres généraux de la tâche Analyse à la demande via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche que vous souhaitez configurer.
3. Dans le panneau de détails du nœud enfant, cliquez sur le lien **Propriétés**.

La fenêtre **Paramètres de la tâche** s'ouvre.

► *Pour ouvrir la fenêtre des paramètres de la zone d'analyse via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau de détails du nœud sélectionné.

La fenêtre **Configuration de la zone d'analyse** s'ouvre.

## Création et configuration d'une tâche d'analyse à la demande

Vous pouvez créer des tâches définies par l'utilisateur pour un seul serveur dans le nœud **Analyse à la demande**.

Les autres composants de Kaspersky Security for Windows Server ne prévoient pas la création de tâches définies par l'utilisateur.

► *Pour créer et configurer une tâche d'analyse à la demande :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Analyse à la demande**.

2. Choisissez l'option **Ajouter une tâche**.

La fenêtre **Ajouter une tâche** s'ouvre.

3. Configurez les paramètres de la tâche suivants :

- **Nom** : nom de la tâche, 100 caractères maximum, peut contenir n'importe quel caractère sauf " \* < > & \ : |

Vous ne pouvez pas enregistrer une nouvelle tâche ou passer à la configuration des paramètres de la nouvelle tâche sous les onglets **Planification**, **Avancé** et **Exécuter en tant que** si le nom de la tâche n'est pas défini.

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

- **Utiliser l'analyse heuristique.**

La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

Si la case est cochée, l'analyse heuristique est activée.

Si la case est décochée, l'analyse heuristique est désactivée.

Cette case est cochée par défaut.

- **Exécuter la tâche en arrière-plan.**

La case modifie la priorité de la tâche.

Si la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et le système de fichiers du serveur par les autres tâches de Kaspersky Security for Windows Server ou les autres applications. Par conséquent la vitesse d'exécution de la tâche diminue quand la charge augmente et inversement.

Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Security for Windows Server et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

Cette case est décochée par défaut.

- **Appliquer la zone de confiance.**

La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche.

Si la case est cochée, Kaspersky Security for Windows Server ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche.

Si la case est décochée, Kaspersky Security for Windows Server ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche.

Cette case est cochée par défaut.

- **Considérer l'exécution de la tâche comme une analyse des zones critiques.**

La case modifie la priorité de la tâche : active ou désactive l'enregistrement des événements dans le journal *Analyse des zones critiques* et l'actualisation de l'état de la protection du serveur. Kaspersky Security Center évalue la sécurité du ou des serveurs sur la base des résultats des performances des tâches portant l'état *Analyse des zones critiques*. La case n'est pas accessible dans les propriétés des tâches locales du système ou définies par l'utilisateur dans Kaspersky Security for Windows Server. Vous pouvez modifier ce paramètre uniquement du côté de Kaspersky Security Center.

Si la case est cochée, le Serveur d'administration consigne l'événement Analyse des zones critiques réalisée et actualise l'état de la protection du serveur sur la base des résultats de l'exécution de la tâche. La priorité de la tâche d'analyse est élevée.

Si la case est décochée, la tâche d'analyse est exécutée selon une priorité faible.

La case est cochée par défaut pour les tâches d'analyse à la demande définie par l'utilisateur.

- **Utiliser KSN pour l'analyse.**

La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

Si la case est décochée, la tâche d'analyse à la demande n'utilise pas les services du KSN.

Cette case est cochée par défaut.

4. Configurez les paramètres de planification du lancement des tâches (cf. section "Paramètres de configuration de la planification du lancement de la tâche" à la page [158](#)) sous les onglets **Planification** et **Avancé**.

5. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section "Définition du compte utilisateur pour l'exécution de la tâche" à la page [160](#)).

6. Dans la fenêtre **Ajouter une tâche**, cliquez sur le bouton **OK**.

La tâche d'analyse à la demande définie par l'utilisateur a été créée. Un nœud portant le nom de la nouvelle tâche apparaît dans l'arborescence de la console de l'application. L'opération est enregistrée dans le journal d'audit système (cf. page [214](#)).

7. Sélectionnez **Configurer la zone d'analyse** dans le panneau de détails du nœud sélectionné.

La fenêtre **Configuration de la zone d'analyse** s'ouvre.

8. Dans l'arborescence des ressources de fichier du serveur ou dans la liste, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.

9. Sélectionnez un des niveaux de sécurité prédéfinis (cf. section "A propos des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande" à la page [481](#)) ou configurez manuellement les paramètres d'analyse (cf. section "Configuration manuelle des paramètres de sécurité" à la page [510](#)).



10. Cliquez sur **Enregistrer** dans la fenêtre **Configuration de la zone d'analyse**.

Les paramètres configurés seront appliqués lors de la prochaine exécution de la tâche.

## Zone d'analyse dans les tâches d'analyse à la demande

Cette section fournit des informations sur la création et l'utilisation d'une zone d'analyse dans les tâches d'analyse à la demande.

### Dans cette section

Configuration des paramètres de l'affichage des ressources de fichier réseau .....	<a href="#">506</a>
Constitution d'une zone d'analyse .....	<a href="#">506</a>
Inclusion des objets réseau dans la zone d'analyse .....	<a href="#">508</a>
Création d'une zone d'analyse virtuelle .....	<a href="#">509</a>

### Configuration des paramètres de l'affichage des ressources de fichier réseau

► *Pour choisir le mode d'affichage des ressources de fichier réseau lors de la configuration des paramètres de la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Déployez la liste déroulante de la section supérieure gauche de la fenêtre. Exécutez une des actions suivantes :
  - Choisissez le point **Afficher sous forme d'arborescence** si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une arborescence.
  - Choisissez le point **Afficher sous forme de liste**, si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une liste.

Par défaut les ressources de fichier réseau du serveur protégé s'affichent sous la forme d'une liste.

3. Cliquez sur le bouton **Enregistrer**.

La fenêtre Configuration de la zone d'analyse se ferme. Les paramètres de la tâche définis seront appliqués.

### Constitution d'une zone d'analyse

Si vous administrez Kaspersky Security for Windows Server sur le serveur protégé à distance via la console de l'application installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur le serveur protégé pour consulter les dossiers du serveur.

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Si vous modifiez la zone d'analyse dans les tâches Analyse au démarrage du système d'exploitation et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la restauration de Kaspersky Security for Windows Server (**Démarrer > Programmes > Kaspersky Security for Windows Server > Modification ou suppression de Kaspersky Security for Windows Server**). Dans l'assistant d'installation, sélectionnez l'option **Réparation des composants installés**, cliquez sur **Suivant**, puis cochez la case **Rétablir les paramètres recommandés de l'application**.

La procédure de constitution d'une zone d'analyse dans les tâches d'analyse à la demande dépend du type d'affichage des ressources de fichier réseau (cf. section "Configuration des paramètres de l'affichage des ressources de fichier réseau" à la page [506](#)). Vous pouvez configurer l'affichage des ressources de fichier réseau sous la forme d'une liste (est appliqué par défaut) ou sous la forme d'une arborescence.

► *Pour composer une zone d'analyse au départ l'arborescence des ressources de fichier réseau, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Dans la partie gauche de la fenêtre ouverte déployez l'arborescence des ressources de fichier réseau pour afficher tous les nœuds et les nœuds enfants.
3. Exécutez les actions suivantes :
  - Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.
  - Pour inclure certaines entrées dans la zone d'analyse, décochez la case **Poste de travail** et procédez comme suit :
    - Si vous souhaitez inclure dans la zone d'analyse 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 dans la zone d'analyse, développez le nœud 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:**, développez le nœud **Disques amovibles** et cochez la case en regard du disque **F:**.
    - Si vous souhaitez inclure dans la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case en regard de ce dossier ou de ce fichier.
4. Cliquez sur le bouton **Enregistrer**.

La fenêtre Configuration de la zone d'analyse se ferme. Les paramètres de la tâche définis seront enregistrés.

► *Pour créer une zone d'analyse à l'aide de la liste des ressources de fichier réseau, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Pour inclure certaines entrées dans la zone d'analyse, décochez la case **Poste de travail** et procédez comme suit :
  - a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.
  - b. Dans le menu contextuel, choisissez l'option **Ajouter une zone d'analyse**.
  - c. Dans la fenêtre **Ajout d'une zone d'analyse** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter à la zone d'analyse :
    - **Zone prédéfinie**, si vous voulez ajouter une des zones prédéfinies sur un serveur protégé. Puis,

dans la liste déroulante, choisissez la zone d'analyse nécessaire.

- **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone d'analyse un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone requise en cliquant sur le bouton **Parcourir**.
- **Fichier**, si vous voulez insérer dans la zone d'analyse uniquement un fichier distinct sur le disque. Puis choisissez la zone requise en cliquant sur le bouton **Parcourir**.

**Vous ne pouvez pas ajouter un objet à la zone d'analyse s'il est déjà ajouté en tant qu'exclusion de la zone de protection.**

3. Pour exclure certaines entrées de la zone d'analyse, décochez les cases en regard des noms de ces entrées ou réalisez les opérations suivantes :
  - a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.
  - b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.
  - c. Dans la fenêtre **Ajouter une exclusion**, choisissez le type de l'objet que vous voulez ajouter à titre d'exclusion de la zone d'analyse, de la même manière que l'ajout d'un objet à la zone d'analyse.
4. Pour modifier la zone d'analyse ou une exclusion ajoutée, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Modifier la zone**.
5. Pour masquer la zone d'analyse ou une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Supprimer de la liste**.

**La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.**

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre Configuration de la zone d'analyse se ferme. Les paramètres de la tâche définis seront enregistrés.

## Inclusion des objets réseau dans la zone d'analyse

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

**Vous ne pouvez pas analyser les dossiers réseau en cas d'utilisation du compte système.**

► *Pour ajouter un emplacement réseau à la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Dans le menu contextuel du nœud **Réseau** :
  - Choisissez l'option **Ajouter un dossier de réseau** si vous souhaitez ajouter un dossier réseau à la

zone d'analyse.

- Choisissez l'option **Ajouter un fichier de réseau** si vous souhaitez ajouter un fichier réseau à la zone d'analyse.
4. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et appuyez sur la touche **ENTER**.
  5. Cochez la case en regard du nom de l'objet réseau ajouté afin de l'inclure dans la zone d'analyse.
  6. Le cas échéant, modifiez les paramètres de sécurité de l'objet réseau ajouté.
  7. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

## Création d'une zone d'analyse virtuelle

Vous pouvez insérer dans la zone d'analyse des disques, des dossiers et des fichiers dynamiques ou créer une zone d'analyse virtuelle.

Vous pouvez ajouter à la zone de protection/d'analyse des disques virtuels, des dossiers ou des fichiers distincts, uniquement si la zone de protection/d'analyse s'affiche sous la forme d'une arborescence de ressources de fichier (cf. section "Configuration des paramètres de l'affichage des ressources de fichier réseau" à la page [506](#)).

► *Pour ajouter un disque virtuel à la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Dans l'arborescence des ressources de fichier serveur, ouvrez le menu contextuel du nœud **Disques virtuels**, cliquez sur **Ajouter une disque virtuel**, puis sélectionnez le nom du disque virtuel créé dans la liste des noms disponibles.
4. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone d'analyse.
5. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

► *Pour ajouter un dossier ou un fichier virtuel à la zone d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Dans l'arborescence des ressources fichiers du serveur, ouvrez le menu contextuel du nœud auquel vous souhaitez ajouter le répertoire ou le fichier et sélectionnez l'une des options suivantes :
  - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone d'analyse.
  - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone d'analyse.
4. Dans le champ, saisissez le nom du dossier ou du fichier.

5. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone d'analyse.
6. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

## Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour un nœud ou un élément sélectionné dans l'arborescence ou dans la liste des ressources de fichier réseau du serveur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Dans l'arborescence ou dans la liste des ressources de fichier réseau du serveur, sélectionnez le nœud ou l'élément pour lequel vous souhaitez sélectionner un niveau de sécurité prédéfini.
3. Assurez-vous que le nœud ou l'élément sélectionné se trouve dans la zone d'analyse.
4. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez le niveau que vous souhaitez appliquer.

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

5. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

## Configuration manuelle des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé** (cf. section "Niveaux de sécurité prédéfinis" à la page [251](#)).

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers du serveur.

Lorsque vous utilisez l'arborescence des ressources de fichier réseau, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds enfants. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

► *Pour configurer manuellement les paramètres de sécurité :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le nœud ou l'élément dont vous souhaitez configurer les paramètres de sécurité.

Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité (cf. section "A propos des modèles de paramètres de sécurité" à la page [164](#)) à un nœud ou un élément sélectionné dans la zone d'analyse.

3. Configurez les paramètres de sécurité requis pour le nœud ou l'élément sélectionné en fonction de vos exigences sous les onglets suivants :
  - Paramètres généraux (cf. section "Configuration des règles prédéfinies d'une tâche" à la page [511](#))
  - Actions (cf. section "Configuration des actions" à la page [514](#))
  - Optimisation (cf. section "Configuration de l'optimisation" à la page [515](#))
  - Stockage hiérarchique
4. Cliquez sur **Enregistrer** dans la fenêtre **Configuration de la zone d'analyse**.

Les paramètres de la nouvelle zone d'analyse sont enregistrés.

## Dans cette section

Configuration des paramètres de tâche généraux .....	<a href="#">511</a>
Configuration des actions .....	<a href="#">514</a>
Configuration de l'optimisation.....	<a href="#">515</a>
Configuration du stockage hiérarchique .....	<a href="#">517</a>

## Configuration des paramètres de tâche généraux

► *Pour configurer les paramètres de sécurité générale d'une tâche d'analyse à la demande :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Analyser les objets**, indiquez les types d'objets que vous souhaitez inclure dans la zone d'analyse :
  - **Objets à analyser**
    - **Tous les objets**  
Kaspersky Security for Windows Server analyse tous les objets.
    - **Objets analysés en fonction du format**  
Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base du format du fichier.  
  
Kaspersky Lab compile la liste des formats. Elle figure dans les bases de données de Kaspersky Security for Windows Server.
    - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**  
Kaspersky Security for Windows Server analyse uniquement les fichiers infectables sur la base de l'extension du fichier.  
  
Kaspersky Lab compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Security for Windows Server.

- **Objets analysés en fonction de la liste d'extensions indiquée**

Kaspersky Security for Windows Server analyse les fichiers sur la base de leur extension. Vous pouvez personnaliser manuellement la liste des extensions des fichiers à analyser en cliquant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.
  - **Analyser les secteurs d'amorçage et la partition MBR**

Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

Si la case est cochée, Kaspersky Security for Windows Server analyse les secteurs et les zones d'amorce sur les disques durs et les disques amovibles du serveur.

Cette case est cochée par défaut.
  - **Analyser les flux NTFS alternatifs**

Analyse des flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

Si la case est cochée, l'application analyse un objet probablement infecté et tous les flux NTFS associés à cet objet.

Si la case est décochée, l'application analyse uniquement l'objet qui a été détecté et considéré comme probablement infecté.

Cette case est cochée par défaut.
4. Dans le section **Optimisation**, cochez ou décochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.
- La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Security for Windows Server a identifiés comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.
- Si la case est cochée, Kaspersky Security for Windows Server analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.
- Si la case est décochée, vous pouvez décider si vous souhaitez analyser et protéger uniquement les nouveaux fichiers ou tous les fichiers, quel que soit leur état de modification.
- La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Protection maximale** ou **Recommandé**, la case est décochée.

Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.

5. Dans la section **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
- **Toutes les/ Les nouvelles archives**

Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives lors

de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Toutes les / Les nouvelles archives SFX**

Analyse des archives auto-extractibles.

Si la case est cochée, Kaspersky Security for Windows Server analyse les archives SFX.

Si la case est décochée, Kaspersky Security for Windows Server ignore les archives SFX lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données d'emails**

Analyse des fichiers des bases de données de messagerie de Microsoft Outlook et Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers des bases de données de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers des bases de données de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets compactés**

Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers exécutables compactés par des logiciels de compression.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

La valeur par défaut dépend du niveau de protection sélectionné.

- **Tous les / Les nouveaux messages de texte brut**

Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers aux formats de messagerie.

Si la case est décochée, Kaspersky Security for Windows Server ignore les fichiers aux formats de messagerie lors de l'analyse.

La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**

Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

Si la case est cochée, Kaspersky Security for Windows Server analyse les objets intégrés au fichier.

Si la case est décochée, Kaspersky Security for Windows Server ignore les objets intégrés au fichier lors de l'analyse.



La valeur par défaut dépend du niveau de protection sélectionné.

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration des actions

- *Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Analyse à la demande :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Sélectionnez l'onglet **Actions**.
3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Désinfecter.**
- **Désinfecter. Supprimer si la désinfection est impossible.**
- **Supprimer.**
- **Exécuter l'action recommandée.**

4. Sélectionnez l'action à exécuter sur les objets probablement infectés :

- **Informé uniquement.**

En cas de détection de ce mode, Kaspersky Security for Windows Server n'interdit pas l'accès aux objets détectés, ni n'effectue d'actions sur ces objets. L'événement suivant est enregistré dans le journal d'exécution de la tâche : *Objet non désinfecté. Raison : aucune action n'a été effectuée pour neutraliser l'objet détecté en raison des paramètres définis par l'utilisateur.* L'événement spécifie toutes les informations disponibles sur l'objet détecté.

Le mode **Informé uniquement** doit être configuré séparément pour chaque zone d'analyse ou de protection. Ce mode n'est utilisé par défaut sur aucun des niveaux de sécurité. Si vous sélectionnez ce mode, Kaspersky Security for Windows Server redéfinit automatiquement le niveau de sécurité sur **Personnalisé**.

- **Quarantaine.**
- **Supprimer.**
- **Exécuter l'action recommandée.**

5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
  - a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

Si la case est cochée, vous pouvez indépendamment définir une action principale et secondaire pour chaque type d'objet détecté en cliquant sur le bouton **Configuration** en regard de la case. De plus, Kaspersky Security for Windows Server ne permet pas d'ouvrir ou d'exécuter un objet infecté, quel que soit votre choix.

Si la case est décochée, Kaspersky Security for Windows Server exécute les actions sélectionnées dans les sections **Actions à exécuter sur les objets infectés et autres** et **Actions à exécuter sur les objets probablement infectés** des types d'objets nommés, respectivement.

Cette case est décochée par défaut.
  - b. Cliquez sur le bouton **Configuration**.
  - c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (si la première échoue) pour chaque type d'objet détecté.
  - d. Cliquez sur le bouton **OK**.
6. Choisissez l'action à exécuter sur les objets composés qui ne peuvent être désinfectés : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**

La case active ou désactive la suppression forcée du fichier composé parent en cas de détection d'un objet intégré malveillant, probablement infecté ou autre objet intégré enfant.

Si la case est cochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server force la suppression de tout l'objet composé parent en cas de détection d'un objet intégré malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée d'un fichier parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet enfant détecté (par exemple, si l'objet parent n'est pas modifiable).

Si cette case est décochée et que la tâche est configurée pour supprimer les objets infectés et probablement infectés, Kaspersky Security for Windows Server n'exécute pas l'action indiquée si l'objet parent n'est pas modifiable.
7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration de l'optimisation

### ► Pour configurer la performance de la tâche *Analyse à la demande* :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Sélectionnez l'onglet **Optimisation**.
3. Dans la section **Exclusions** :
  - Cochez ou décochez la case **Exclure les fichiers**.

Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse tous les objets.

Cette case est décochée par défaut.

- Cochez ou décochez la case **Ne pas détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus <https://encyclopedia.kaspersky.com/knowledge/classification/>.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

#### 4. Dans la section **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)**

Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

Si la case est cochée, la durée maximale de l'analyse d'un objet est limitée à la valeur indiquée.

Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Ne pas analyser les objets composés de plus de (Mo)**

Exclut de l'analyse les objets dont la taille est supérieure à la valeur indiquée.

Si la case est cochée, Kaspersky Security for Windows Server ignore pour la recherche de virus les objets composés dont la taille est supérieure à la valeur indiquée.

Si la case est décochée, Kaspersky Security for Windows Server analyse les objets composés sans tenir compte de la taille.

La case est cochée par défaut pour le niveau de sécurité **Performance maximale**.

- **Utiliser la technologie iSwift**

iSwift compare l'identifiant NTFS du fichier, identifiant stocké dans une base de données, avec un identifiant en cours. L'analyse est effectuée uniquement pour les fichiers dont les identifiant ont changé (nouveaux fichiers et fichiers modifiés depuis la dernière analyse des objets système NTFS).

Si la case est cochée, Kaspersky Security for Windows Server analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse des objets système NTFS.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers du système NTFS en ignorant la date de création ou de modification sauf pour les fichiers des dossiers réseau.

Cette case est cochée par défaut.

- **Utiliser la technologie iChecker**

iChecker calcule et enregistre les sommes de contrôle des fichiers analysés. Si un objet est modifié, la somme de contrôle change. L'application compare toutes les sommes de contrôle pendant la tâche d'analyse et analyse uniquement les fichiers nouveaux et modifiés depuis la dernière analyse de fichiers.

Si la case est cochée, Kaspersky Security for Windows Server analyse les fichiers nouveaux et modifiés.

Si la case est décochée, Kaspersky Security for Windows Server analyse les fichiers en ignorant leur date de création ou de modification.

Cette case est cochée par défaut.

5. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Configuration du stockage hiérarchique

- *Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Analyse à la demande :*

1. Ouvrez la fenêtre **Configuration de la zone d'analyse** (à la page [503](#)).
2. Sélectionnez l'onglet **Stockage hiérarchique**.
3. Sélectionnez l'action à exécuter sur les fichiers hors ligne :

- **Ne pas analyser.**
- **Analyser seulement la partie résidente du fichier.**
- **Analyser le fichier en entier.**

Si cette action est sélectionnée, vous pouvez spécifier les options suivantes :

- Cochez ou décochez la case **Uniquement si le fichier a été sollicité durant la période indiquée (jours)** et spécifiez le nombre de jours.
- Cochez ou décochez la case **Ne pas copier le fichier sur le disque dur local si possible.**

4. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

## Analyse des disques amovibles

- *Pour configurer l'analyse des disques amovibles dans la Console de l'application lorsqu'ils sont connectés au serveur protégé, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security** et sélectionnez l'option **Configurer l'analyse des disques amovibles**.

La fenêtre **Analyse des disques amovibles** s'ouvre.

2. Dans la section **Analyse à la connexion**, procédez comme suit :

- Cochez la case **Analyser les disques amovibles à la connexion via USB** si vous souhaitez que Kaspersky Security for Windows Server lance automatiquement l'analyse des disques amovibles à la

connexion.

- Le cas échéant, cochez la case **Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
- Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés et appliqués.

## Statistiques des tâches d'analyse à la demande

Pendant l'exécution de la tâche d'analyse à la demande, vous pouvez consulter des informations détaillées sur le nombre que Kaspersky Security for Windows Server a traité depuis son lancement jusqu'à maintenant.

Ces informations seront accessibles même si vous arrêtez la tâche. Vous pourrez consulter les statistiques de la tâche dans le journal d'exécution de la tâche (cf. section "Consultation des statistiques et informations relatives à la tâche de Kaspersky Security for Windows Server dans les journaux d'exécution des tâches" à la page [218](#)).

► *Pour consulter les statistiques de la tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Les informations relatives aux objets que Kaspersky Security for Windows Server a traités depuis son lancement jusqu'à maintenant sont repris dans le tableau ci-dessous.

Tableau 70. Statistiques des tâches d'analyse à la demande

Champ	Description
<b>Déecté</b>	Nombre d'objets détectés par Kaspersky Security for Windows Server. Par exemple, si Kaspersky Security for Windows Server a découvert une application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
<b>Objets infectés et autres détectés</b>	Nombre d'objets que Kaspersky Security for Windows Server a détectés et classés comme infectés ou nombre de fichiers de logiciels légitimes trouvés qui n'ont pas été exclus de la zone d'action des tâches de la protection en temps réel et des tâches à la demande et qui ont été considérés comme des logiciels légitimes que des intrus peuvent utiliser pour endommager votre ordinateur ou vos données personnelles.
<b>Objets probablement infectés détectés</b>	Nombre d'objets découverts par Kaspersky Security for Windows Server et considérés comme probablement infectés.
<b>Objets non désinfectés</b>	Nombre d'objets que Kaspersky Security for Windows Server n'a pas pu désinfecter pour les raisons suivantes : <ul style="list-style-type: none"> <li>• Le type d'objet détecté ne peut être désinfecté.</li> <li>• une erreur s'est produite lors de la désinfection.</li> </ul>
<b>Objets non placés en quarantaine</b>	Nombre d'objets que Kaspersky Security for Windows Server a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.

Champ	Description
<b>Objets non supprimés</b>	Nombre d'objets que Kaspersky Security for Windows Server a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
<b>Objets non analysés</b>	Nombre d'objets de la zone de protection que Kaspersky Security for Windows Server n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
<b>Objets non sauvegardés</b>	Nombre d'objets dont Kaspersky Security for Windows Server a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
<b>Erreurs de traitement</b>	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
<b>Objets désinfectés</b>	Nombre d'objets désinfectés par Kaspersky Security for Windows Server.
<b>Objets placés en quarantaine</b>	Nombre d'objets placés en quarantaine par Kaspersky Security for Windows Server.
<b>Objets sauvegardés</b>	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Security for Windows Server.
<b>Objets supprimés</b>	Nombre d'objets supprimés par Kaspersky Security for Windows Server.
<b>Objets protégés par mot de passe</b>	Nombre d'objets (archives, par exemple) que Kaspersky Security for Windows Server a ignorés en raison d'une protection par mot de passe.
<b>Objets endommagés</b>	Nombre d'objets que Kaspersky Security for Windows Server a ignorés à cause de leur format endommagé.
<b>Objets traités</b>	Nombre d'objets traités par Kaspersky Security for Windows Server.

Vous pouvez aussi consulter les statistiques des tâches d'analyse à la demande dans le journal d'exécution de la tâche sélectionnée via le lien **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du panneau de détails.

A la fin de l'exécution de la tâche d'analyse à la demande, il est conseillé de traiter manuellement les événements du journal d'exécution de la tâche sous l'onglet **Événements**.

# Zone de confiance

Cette section contient des informations sur la zone de confiance de Kaspersky Security for Windows Server, ainsi que des instructions pour ajouter des objets à la zone de confiance lors de l'exécution des tâches.

## Contenu du chapitre

A propos de la zone de confiance .....	<a href="#">520</a>
Administration de la Zone de confiance via le plug-in d'administration .....	<a href="#">522</a>
Administration de la Zone de confiance via la Console de l'application .....	<a href="#">528</a>

## A propos de la zone de confiance

La zone de confiance est une liste d'exclusions de la zone de protection ou d'analyse que vous pouvez créer et utiliser dans les tâches d'Analyse à la demande, de Protection des fichiers en temps réel, de Protection du trafic, de Monitoring des scripts et de Protection RPC des stockages réseau connectés.

Si vous aviez coché les cases **Ajouter les exclusions recommandées par Microsoft** et **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions** lors de l'installation de Kaspersky Security for Windows Server, celle-ci ajoute à la zone de confiance les fichiers recommandés par Microsoft et Kaspersky Lab pour les tâches de protection en temps réel du serveur.

Vous pouvez créer une zone de confiance dans Kaspersky Security for Windows Server selon les règles suivantes :

- **Processus de confiance.** La zone de confiance contient les objets sollicités par les processus des applications sensibles aux interceptions de fichier.
- **Opérations de sauvegarde.** La zone de confiance reprend les objets sollicités lors des opérations des systèmes de sauvegarde des disques durs sur des périphériques externes.
- **Exclusions.** La zone de confiance reprend les objets, indiqués par leur emplacement et/ou l'objet détectés dans ceux-ci.

Vous pouvez utiliser la zone de confiance dans les tâches de protection des fichiers en temps réel, de protection du trafic, de monitoring des scripts, de protection RPC des stockages réseau connectés, dans les nouvelles tâches d'analyse à la demande et dans toutes les tâches système d'analyse à la demande, à l'exception de la tâche d'analyse de la quarantaine.

Par défaut, la zone de confiance est appliquée dans les tâches Protection des fichiers en temps réel et Analyse à la demande.

Vous pouvez exporter la liste des règles de composition de la zone de confiance dans un fichier de configuration au format XML afin de pouvoir l'importer par la suite dans une version de Kaspersky Security for Windows Server installée sur un autre ordinateur.

### Processus de confiance

Applicable aux tâches Protection des fichiers en temps réel et Protection du trafic.

Certaines applications du serveur peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par Kaspersky Security for Windows Server. 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 des fichiers consultés 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 de la Protection des fichiers en temps réel certains fichiers du système d'exploitation Microsoft Windows et les fichiers des applications de Microsoft qui ne peuvent être infectés. Les noms de certains d'entre eux sont repris sur le site Internet de Microsoft <https://www.microsoft.com/en-us/> (code de l'article : KB822158).

Vous pouvez activer ou désactiver l'application des processus de confiance dans la zone de confiance.

Si le fichier exécutable du processus change, par exemple s'il est actualisé, Kaspersky Security for Windows Server l'exclut de la liste des processus de confiance.

L'application n'utilise pas la valeur du chemin vers le fichier sur un serveur protégé pour faire confiance au processus. Le chemin d'accès au fichier sur le serveur protégé est appliqué seulement pour la recherche du fichier et le calcul de sa somme de contrôle, ainsi que pour informer l'utilisateur sur la source du fichier exécutable.

### Opérations de sauvegarde

Applicable aux tâches de protection en temps réel du serveur.

Pendant la sauvegarde des données des disques durs sur des périphériques externes, vous pouvez désactiver la protection des objets sollicités durant les opérations de sauvegarde. Kaspersky Security for Windows Server n'analyse pas les objets que l'application de copie de sauvegarde ouvre en lecture avec l'indice FILE\_FLAG\_BACKUP\_SEMANTICS.

### Exclusions

Applicable aux tâches Protection des fichiers en temps réel, Protection du trafic, Protection RPC des stockages réseau connectés et Analyse à la demande.

Vous pouvez sélectionner les tâches dans lesquelles vous souhaitez appliquer chacune des exclusions ajoutées à la zone de confiance. Vous pouvez également exclure des objets de l'analyse dans les paramètres du niveau de sécurité de chaque tâche de Kaspersky Security for Windows Server.

Vous pouvez ajouter à la zone de confiance des objets en fonction de leur emplacement sur le serveur ou en fonction du nom ou du masque de nom de l'objet détecté dans ces objets. Vous pouvez également utiliser les deux paramètres.

Sur la base de l'exclusion, Kaspersky Security for Windows Server peut ignorer des objets dans les tâches indiquées en fonction des paramètres suivants :

- objets spécifiés détectables selon le nom ou le masque du nom dans les zones désignées du serveur ou des périphériques de stockage NAS ;
- tous les objets détectables dans les zones désignées du serveur ou du périphérique de stockage NAS ;
- objets détectables désignés selon le nom ou le masque de nom dans toute la zone de protection ou d'analyse.



# Administration de la Zone de confiance via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration de la zone de confiance pour un seul ou pour l'ensemble des serveurs du réseau.

## Dans cette section

Navigation .....	<a href="#">522</a>
Configuration des paramètres de la Zone de confiance via le plug-in d'administration .....	<a href="#">523</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Administration de l'application via Kaspersky Security Center .....	<a href="#">522</a>
Ouverture de la fenêtre des propriétés de la Zone de confiance .....	<a href="#">523</a>

## Administration de l'application via Kaspersky Security Center

► *Pour ouvrir une Zone de confiance via une stratégie de Kaspersky Security Center :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Complémentaire**.
6. Cliquez sur le bouton **Configuration** de la sous-section **Zone de confiance**.

La fenêtre **Zone de confiance** s'ouvre.

Configurez la stratégie en fonction des besoins.

Si le serveur est administré par une stratégie active de Kaspersky Security Center et que cette stratégie interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés via la Console de l'application.

## Ouverture de la fenêtre des propriétés de la Zone de confiance

► Pour configurer la Zone de confiance dans la fenêtre des propriétés de l'application, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <nom du serveur>** à l'aide d'une des méthodes suivantes :
  - Double-clic sur le nom du serveur protégé.
  - Sélectionnez l'option **Propriétés** dans le menu contextuel du serveur protégé.

La fenêtre **Propriétés : <nom du serveur>** s'ouvre.

5. Dans la section **Applications**, sélectionnez **Kaspersky Security for Windows Server**.
6. Cliquez sur le bouton **Propriétés**.  
La fenêtre **Configuration de Kaspersky Security for Windows Server** s'ouvre.
7. Sélectionnez la section **Complémentaire**.
8. Cliquez sur le bouton **Configuration** de la sous-section **Zone de confiance**.

La fenêtre **Zone de confiance** s'ouvre.

Configurez la zone de confiance en fonction des besoins.

## Configuration des paramètres de la Zone de confiance via le plug-in d'administration

La zone de confiance est appliquée par défaut à toutes les nouvelles tâches et stratégies.

Pour configurer les paramètres de la zone de confiance, procédez comme suit :

1. Définissez les objets que Kaspersky Security for Windows Server va ignorer (cf. Section "Ajout d'une exclusion" à la page [524](#)) lors de l'exécution de la tâche sous l'onglet **Exclusions**.
2. Définissez les processus que Kaspersky Security for Windows Server va ignorer (cf. Section "Ajout de processus de confiance" à la page [525](#)) lors de l'exécution de la tâche sous l'onglet **Processus de confiance**.
3. Appliquez le masque not-a-virus (cf. section "Application du masque not-a-virus" à la page [527](#)).

### Dans cette section

Ajout d'une exclusion .....	<a href="#">524</a>
Ajout de processus de confiance .....	<a href="#">525</a>
Application du masque not-a-virus .....	<a href="#">527</a>

## Ajout d'une exclusion

► Pour ajouter une exclusion à la Zone de confiance via une stratégie de Kaspersky Security Center :

1. Ouvrez la fenêtre **Zone de confiance** (cf. section "**Administration de l'application via Kaspersky Security Center**" à la page [522](#)).
2. Sous l'onglet **Exclusions**, indiquez les objets qui seront ignorés par Kaspersky Security for Windows Server lors de l'analyse :
  - Pour ajouter les exclusions recommandées, cliquez sur le bouton **Ajouter les exclusions recommandées**.

Quand vous cliquez sur ce bouton, les exclusions recommandées par Microsoft Corporation et celles recommandées par Kaspersky Lab sont ajoutées à la liste des exclusions.
  - Pour importer des exclusions, cliquez sur le bouton **Importer** et dans la fenêtre qui s'ouvre, sélectionnez les fichiers que Kaspersky Security for Windows Server va considérer comme des fichiers de confiance.
  - Si vous souhaitez indiquer manuellement la condition qui, une fois satisfaite, permettra de considérer un fichier comme un fichier de confiance, cliquez sur le bouton **Ajouter**.

La fenêtre **Exclusion** s'ouvre.

3. Dans la section **L'objet ne sera pas analysé lorsque les conditions suivantes seront remplies**, spécifiez les objets à exclure de la zone de protection/zone d'analyse et les objets à exclure parmi les objets détectables :
  - Si vous souhaitez exclure un objet de la zone de protection ou d'analyse :

- a. Cochez la case **Objet à analyser**.

Ajoute un fichier, un dossier, un disque ou un fichier script à une exclusion.

Si la case est cochée, Kaspersky Security for Windows Server ignore la zone, le fichier, le dossier, le disque ou le fichier script prédéfini(e) spécifié(e) lors de l'analyse à l'aide du composant Kaspersky Security for Windows Server sélectionné dans la section **Zone d'application de la règle**.

Cette case est décochée par défaut.

- b. Cliquez sur le bouton **Modifier**.

La fenêtre **Sélectionnez un objet** s'ouvre.

- c. Renseignez l'objet que vous souhaitez exclure de la zone d'analyse.

Vous pouvez utiliser les caractères spéciaux ? et \* lors de la spécification des objets.

- d. Cliquez sur le bouton **OK**.
  - e. Cochez la case **Appliquer également aux sous-dossiers** si vous souhaitez exclure tous les fichiers et dossiers enfants de l'objet indiqué de la protection ou de la zone d'analyse.
- Si vous spécifiez le nom d'un objet détectable :
    - a. Cochez la case **Objets à détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste

des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- b. Cliquez sur le bouton **Modifier**.

La fenêtre **Liste des objets à détecter** s'ouvre.

- c. Renseignez le nom ou le masque du nom de l'objet détectable en fonction de la classification de l'encyclopédie des virus.
- d. Cliquez sur **Ajouter**.
- e. Cliquez sur le bouton **OK**.

4. Dans la section **Zone d'application de la règle**, cochez les cases en regard des noms des tâches auxquelles l'exclusion doit être appliquée.

Nom de la tâche de Kaspersky Security for Windows Server dans laquelle la règle est appliquée.

5. Cliquez sur le bouton **OK**.

L'exclusion est affichée dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

## Ajout de processus de confiance

► *Pour ajouter un ou plusieurs processus à la liste des processus de confiance :*

1. Ouvrez la fenêtre **Zone de confiance** (cf. section "Administration de l'application via Kaspersky Security Center" à la page [522](#)).
2. Ouvrez l'onglet **Processus de confiance**.
3. Cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers** pour éviter l'analyse des opérations de lecture de fichiers.

La case active ou désactive l'analyse des opérations de lecture des fichiers si ces opérations sont réalisées par des outils de copie de sauvegarde installés sur le serveur.

Si la case est cochée, Kaspersky Security for Windows Server ignore les opérations de lecture de fichiers réalisées par les outils de copie de sauvegarde installés sur le serveur.

Si la case est décochée, Kaspersky Security for Windows Server analyse les opérations de lecture des fichiers exécutées par les outils de copie de sauvegarde installés sur le serveur.

Cette case est cochée par défaut.

4. Cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** pour éviter l'analyse des opérations sur les fichiers pour les processus de confiance.

La case active ou désactive l'analyse des actions des processus de confiance sur les fichiers.

Si la case est cochée, Kaspersky Security for Windows Server ignore les opérations des processus de confiance sur les fichiers lors de l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse les opérations des processus de confiance sur les fichiers.

Cette case est décochée par défaut.

5. Cliquez sur **Ajouter**.
6. Sélectionnez une des options suivantes dans le menu contextuel du bouton :

- **Processus multiples.**

Configurez les paramètres suivants dans la fenêtre **Ajout de processus de confiance** qui s'ouvre :

- a. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.

- b. **Utiliser le hash du fichier de processus pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte pour définir l'état de confiance du processus.

Cette case est cochée par défaut.

- c. Cliquez sur le bouton **Parcourir** pour ajouter des données sur la base de processus exécutables.
- d. Dans la fenêtre qui s'ouvre, sélectionnez un fichier exécutable.

Vous pouvez ajouter un seul fichier exécutable à la fois. Répétez les étapes c-d pour ajouter d'autres fichiers exécutables.

- e. Cliquez sur le bouton **Processus** pour ajouter des données sur la base de processus en cours.
- f. Dans la fenêtre qui s'ouvre, sélectionnez des processus. Pour sélectionner plusieurs processus, maintenez le bouton **CTRL** enfoncé.
- g. Cliquez sur le bouton **OK**.

Le compte utilisateur sous les privilèges duquel la tâche Protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur le serveur où Kaspersky Security for Windows Server est installé afin de pouvoir consulter la liste des processus actifs. Vous pouvez trier les processus dans la liste des processus actifs selon le nom du fichier, l'identificateur de processus (PID) ou le chemin d'accès au fichier exécutable du processus sur le serveur local. Vous pouvez sélectionner des processus dans la liste des processus en cours d'exécution en cliquant sur le bouton **Processus** uniquement si vous utilisez la Console de l'application sur un serveur local ou dans les paramètres de l'hôte indiqué via Kaspersky Security Center.

- **Un seul processus basé sur le nom et le chemin du fichier.**

Dans la fenêtre **Ajout d'un processus** qui s'ouvre, procédez comme suit :

- a. Saisissez un chemin d'accès au fichier exécutable (y compris le nom du fichier).
  - b. Cliquez sur le bouton **OK**.
- **Un seul processus basé sur les propriétés...**

Configurez les paramètres suivants dans la fenêtre **Ajout d'un processus de confiance** qui s'ouvre :

    - a. Cliquez sur le bouton **Parcourir** et sélectionnez un processus.
    - b. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.
    - c. **Utiliser le hash du fichier de processus pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte pour définir l'état de confiance du processus.

Cette case est cochée par défaut.
    - d. Cliquez sur le bouton **OK**.

Pour ajouter le processus sélectionné à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

7. Dans la fenêtre **Ajout de processus de confiance**, cliquez sur le bouton **OK**.

Le fichier ou le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

## Application du masque not-a-virus

Le masque not-a-virus permet d'ignorer les fichiers logiciels et les ressources internet légitimes, qui peuvent être considérés comme nuisibles pendant l'analyse. Le masque concerne les tâches suivantes :

- Protection des fichiers en temps réel.
- Analyse à la demande.
- Monitoring des scripts.
- Protection RPC des stockages réseau connectés.
- Protection du trafic.

Si le masque n'est pas ajouté à la liste d'exclusions, Kaspersky Security for Windows Server applique les actions spécifiées dans les paramètres d'exécution de la tâche pour les ressources logicielles ou Internet qui entrent dans

cette catégorie.

► *Pour appliquer le masque not-a-virus, procédez comme suit :*

1. Ouvrez la fenêtre **Zone de confiance** (cf. section "Administration de l'application via Kaspersky Security Center" à la page [522](#)).
2. Dans la colonne **Objets à détecter** de l'onglet **Exclusions**, faites défiler la liste et sélectionnez la ligne avec la valeur **not-a-virus:\*** si la case est décochée.
3. Cliquez sur le bouton **OK**.

Une nouvelle configuration est appliquée.

## Administration de la Zone de confiance via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration de la Zone de confiance sur un serveur local.

### Dans cette section

Application de la Zone de confiance aux tâches dans la Console de l'application .....	<a href="#">528</a>
Configuration des paramètres de la Zone de confiance dans la Console de l'application .....	<a href="#">529</a>

## Application de la Zone de confiance aux tâches dans la Console de l'application

La zone de confiance est appliquée par défaut dans les tâches de protection des fichiers en temps réel, dans les tâches définies par l'utilisateur nouvellement créées d'analyse à la demande et dans toutes les tâches système d'analyse à la demande, à l'exception de la tâche d'analyse de la quarantaine.

Dès que la zone de confiance est activée/désactivée, les exclusions définies dans celle-ci seront ou ne seront plus appliquées dans les tâches exécutées immédiatement.

► *Pour activer ou désactiver l'utilisation d'une Zone de confiance dans les tâches de Kaspersky Security for Windows Server, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer l'utilisation de la Zone de confiance.
2. Choisissez l'option **Propriétés**.  
La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et réalisez une des opérations suivantes :
  - Si vous souhaitez utiliser une zone de confiance dans la tâche, cochez la case **Appliquer la zone de confiance**.

- Si vous ne souhaitez pas utiliser une zone de confiance, décochez la case **Appliquer la zone de confiance**.
4. Pour configurer les paramètres de la Zone de confiance, cliquez sur le lien dans le nom de la case **Appliquer la zone de confiance**.  
La fenêtre **Zone de confiance** s'ouvre.
  5. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de la tâche** pour enregistrer les modifications.

## Configuration des paramètres de la Zone de confiance dans la Console de l'application

Pour configurer les paramètres de la zone de confiance, procédez comme suit :

1. Définissez les objets que Kaspersky Security for Windows Server va ignorer (cf. Section "Ajout d'une exclusion à la Zone de confiance" à la page [529](#)) lors de l'exécution de la tâche sous l'onglet **Exclusions**.
2. Définissez les processus que Kaspersky Security for Windows Server va ignorer (cf. Section "Processus de confiance" à la page [531](#)) lors de l'analyse sous l'onglet **Processus de confiance**.
3. Appliquez la Zone de confiance aux tâches de l'application (cf. section "Application de la Zone de confiance aux tâches dans la Console de l'application" à la page [528](#)).
4. Appliquez le masque not-a-virus (cf. section "Application du masque not-a-virus" à la page [533](#)).

### Dans cette section

Ajout d'une exclusion à la zone de confiance.....	<a href="#">529</a>
Processus de confiance.....	<a href="#">531</a>
Application du masque not-a-virus .....	<a href="#">533</a>

## Ajout d'une exclusion à la zone de confiance

► *Pour ajouter manuellement une exclusion à la zone de confiance via la Console de l'application, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.  
La fenêtre **Zone de confiance** s'ouvre.
3. Sélectionnez l'onglet **Exclusions**.
4. Cliquez sur **Ajouter**.  
La fenêtre **Exclusion** s'ouvre.
5. Dans la section **L'objet ne sera pas analysé lorsque les conditions suivantes seront remplies**, spécifiez les objets à exclure de la zone de protection/zone d'analyse et les objets à exclure parmi les objets détectables :
  - Si vous souhaitez exclure un objet de la zone de protection ou d'analyse :



- a. Cochez la case **Objet à analyser**.

Ajoute un fichier, un dossier, un disque ou un fichier script à une exclusion.

Si la case est cochée, Kaspersky Security for Windows Server ignore la zone, le fichier, le dossier, le disque ou le fichier script prédéfini(e) spécifié(e) lors de l'analyse à l'aide du composant Kaspersky Security for Windows Server sélectionné dans la section **Zone d'application de la règle**.

Cette case est décochée par défaut.

- b. Cliquez sur le bouton **Modifier**.

La fenêtre **Sélectionnez un objet** s'ouvre.

- c. Renseignez l'objet que vous souhaitez exclure de la zone d'analyse.

Vous pouvez utiliser les caractères spéciaux ? et \* lors de la spécification des objets.

- d. Cliquez sur le bouton **OK**.

- e. Cochez la case **Appliquer également aux sous-dossiers** si vous souhaitez exclure tous les fichiers et dossiers enfants de l'objet indiqué de la protection ou de la zone d'analyse.

- Si vous spécifiez le nom d'un objet détectable :

- a. Cochez la case **Objets à détecter**.

Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus.

Si la case est cochée, Kaspersky Security for Windows Server ignore les objets à détecter indiqués pendant l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server détecte tous les objets indiqués par défaut dans l'application.

Cette case est décochée par défaut.

- b. Cliquez sur le bouton **Modifier**.

La fenêtre **Liste des objets à détecter** s'ouvre.

- c. Renseignez le nom ou le masque du nom de l'objet détectable en fonction de la classification de l'encyclopédie des virus.
- d. Cliquez sur **Ajouter**.
- e. Cliquez sur le bouton **OK**.

6. Dans la section **Zone d'application de la règle**, cochez les cases en regard des noms des tâches auxquelles l'exclusion doit être appliquée.

Nom de la tâche de Kaspersky Security for Windows Server dans laquelle la règle est appliquée.

7. Cliquez sur le bouton **OK**.

L'exclusion est affichée dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

## Processus 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 sur le serveur protégé.
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

Si le fichier exécutable d'un processus est modifié, Kaspersky Security for Windows Server l'exclut de la liste des processus de confiance.

► Pour ajouter un ou plusieurs processus à la liste des processus de confiance :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.  
La fenêtre **Zone de confiance** s'ouvre.
3. Ouvrez l'onglet **Processus de confiance**.
4. Cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers** pour éviter l'analyse des opérations de lecture de fichiers.

La case active ou désactive l'analyse des opérations de lecture des fichiers si ces opérations sont réalisées par des outils de copie de sauvegarde installés sur le serveur.

Si la case est cochée, Kaspersky Security for Windows Server ignore les opérations de lecture de fichiers réalisées par les outils de copie de sauvegarde installés sur le serveur.

Si la case est décochée, Kaspersky Security for Windows Server analyse les opérations de lecture des fichiers exécutées par les outils de copie de sauvegarde installés sur le serveur.

Cette case est cochée par défaut.

5. Cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** pour éviter l'analyse des opérations sur les fichiers pour les processus de confiance.

La case active ou désactive l'analyse des actions des processus de confiance sur les fichiers.

Si la case est cochée, Kaspersky Security for Windows Server ignore les opérations des processus de confiance sur les fichiers lors de l'analyse.

Si la case est décochée, Kaspersky Security for Windows Server analyse les opérations des processus de confiance sur les fichiers.

Cette case est décochée par défaut.

6. Cliquez sur **Ajouter**.
7. Sélectionnez une des options suivantes dans le menu contextuel du bouton :
  - **Processus multiples**.  
Configurez les paramètres suivants dans la fenêtre **Ajout de processus de confiance** qui s'ouvre :
    - a. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de**

**confiance.**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.

**b. Utiliser le hash du fichier de processus pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte pour définir l'état de confiance du processus.

Cette case est cochée par défaut.

**c. Cliquez sur le bouton **Parcourir** pour ajouter des données sur la base de processus exécutables.****d. Dans la fenêtre qui s'ouvre, sélectionnez un fichier exécutable.**

Vous pouvez ajouter un seul fichier exécutable à la fois. Répétez les étapes c-d pour ajouter d'autres fichiers exécutables.

**e. Cliquez sur le bouton **Processus** pour ajouter des données sur la base de processus en cours.****f. Dans la fenêtre qui s'ouvre, sélectionnez des processus. Pour sélectionner plusieurs processus, maintenez le bouton **CTRL** enfoncé.****g. Cliquez sur le bouton **OK**.**

Le compte utilisateur sous les privilèges duquel la tâche Protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur le serveur où Kaspersky Security for Windows Server est installé afin de pouvoir consulter la liste des processus actifs. Vous pouvez trier les processus dans la liste des processus actifs selon le nom du fichier, l'identificateur de processus (PID) ou le chemin d'accès au fichier exécutable du processus sur le serveur local. Vous pouvez sélectionner des processus dans la liste des processus en cours d'exécution en cliquant sur le bouton **Processus** uniquement si vous utilisez la Console de l'application sur un serveur local ou dans les paramètres de l'hôte indiqué via Kaspersky Security Center.

- **Un seul processus basé sur le nom et le chemin du fichier.**

Dans la fenêtre **Ajout d'un processus** qui s'ouvre, procédez comme suit :

**a. Saisissez un chemin d'accès au fichier exécutable (y compris le nom du fichier).****b. Cliquez sur le bouton **OK**.**

- **Un seul processus basé sur les propriétés...**

Configurez les paramètres suivants dans la fenêtre **Ajout d'un processus de confiance** qui s'ouvre :

**a. Cliquez sur le bouton **Parcourir** et sélectionnez un processus.****b. Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security for Windows Server détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.

Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est décochée par défaut.

c. **Utiliser le hash du fichier de processus pour le considérer comme de confiance.**

Si la case est cochée, Kaspersky Security 10.1.1 for Windows Server détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte pour définir l'état de confiance du processus.

Cette case est cochée par défaut.

d. Cliquez sur le bouton **OK**.

Pour ajouter le processus sélectionné à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

8. Dans la fenêtre **Ajout de processus de confiance**, cliquez sur le bouton **OK**.

Le fichier ou le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

## Application du masque not-a-virus

Le masque not-a-virus permet d'ignorer les fichiers logiciels et les ressources internet légitimes, qui peuvent être considérés comme nuisibles pendant l'analyse. Le masque concerne les tâches suivantes :

- Protection des fichiers en temps réel.
- Analyse à la demande.
- Monitoring des scripts.
- Protection RPC des stockages réseau connectés.
- Protection du trafic.

Si le masque n'est pas ajouté à la liste d'exclusions, Kaspersky Security for Windows Server applique les actions spécifiées dans les paramètres d'exécution de la tâche pour les ressources logicielles ou Internet qui entrent dans cette catégorie.

► *Pour appliquer le masque not-a-virus, procédez comme suit :*

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.  
La fenêtre **Zone de confiance** s'ouvre.
3. Sélectionnez l'onglet **Exclusions**.

4. Faites défiler la liste et sélectionnez la ligne avec la valeur **not-a-virus:\*** si la case est décochée.
5. Cliquez sur le bouton **OK**.

Une nouvelle configuration est appliquée.

# Protection contre les exploits

Cette section contient les instructions de configuration des paramètres de la protection de la mémoire des processus contre l'exploitation des vulnérabilités.

## Contenu du chapitre

A propos de la Protection contre les exploits .....	<a href="#">535</a>
Administration de la Protection contre les exploits via le plug-in d'administration .....	<a href="#">536</a>
Administration de la Protection contre les exploits via la Console de l'application .....	<a href="#">540</a>
Techniques de protection contre les exploits .....	<a href="#">544</a>

## A propos de la Protection contre les exploits

Kaspersky Security for Windows Server permet de protéger la mémoire des processus contre les exploits. Cette fonction est mise en œuvre via le module Protection contre les exploits. Vous pouvez modifier l'état de l'activité du composant, ainsi que configurer les paramètres de protection des processus contre l'exploitation des vulnérabilités.

Le composant protège la mémoire des processus contre les Exploits à l'aide de l'Agent de protection des processus (ci après Agent) externe intégré au processus protégé.

L'Agent de protection de processus est un module de Kaspersky Security for Windows Server chargé dynamiquement qui s'intègre aux processus protégés en vue de contrôler leur intégrité et de réduire l'impact de l'exploitation des vulnérabilités.

Le fonctionnement de l'Agent à l'intérieur du processus protégé dépend des itérations de lancement et d'arrêt de ce processus : le chargement primaire de l'Agent dans le processus ajouté à la liste des processus protégés est possible seulement au relancement du processus. Le déchargement de l'Agent de processus une fois supprimé de la liste est possible seulement après le relancement du processus.

**Il convient d'arrêter l'Agent avant de le décharger des processus protégés : lors de la suppression du composant Protection contre les exploits, l'application gèle l'environnement et force le déchargement de l'Agent des processus protégés. Si, au cours de la désinstallation du composant, l'agent est inséré dans un des processus protégés, vous devez arrêter le processus affecté. Un redémarrage du serveur peut être nécessaire (par exemple, si le processus système est protégé).**

En cas de détection de signes d'une attaque de l'Exploit sur le processus protégé, Kaspersky Security for Windows Server exécute une des actions suivantes :

- termine le processus lors de la tentative d'exploitation de la vulnérabilité ;
- informe que le processus a été compromis .

Vous pouvez arrêter la protection des processus d'une des manières suivantes :

- supprimer le composant ;

- supprimer le processus de la liste des processus protégés et le relancer.

### Service Kaspersky Security Exploit Prevention

Pour garantir l'efficacité du composant Protection contre les exploits, le service Kaspersky Security Exploit Prevention est requis sur le serveur protégé. Ce service et le module Protection contre les exploits font partie de l'installation recommandée. Lors de l'installation du service sur le serveur protégé, le processus kavfswh est créé et lancé. Celui-ci transmet les informations relatives aux processus protégés depuis le module vers l'Agent de sécurité.

Après l'arrêt du service Kaspersky Security Exploit Prevention, Kaspersky Security for Windows Server continue de protéger les processus qui ont été ajoutés à la liste des processus protégés, puis il est également chargé dans les nouveaux processus ajoutés et applique toutes les techniques disponibles de protection contre les exploits pour protéger la mémoire des processus.

En cas d'arrêt du service Kaspersky Security Exploit Prevention Broker Host, l'application ne reçoit pas les données sur les événements qui se produisent avec les processus protégés (y compris, les données sur les attaques des exploits et l'achèvement des processus). L'Agent ne pourra pas non plus recevoir les données sur les nouveaux paramètres de protection et sur l'ajout des nouveaux processus à la liste des processus protégés.

### Mode de protection contre les exploits

Vous pouvez configurer les actions de réduction de l'impact de l'exploitation des vulnérabilités dans les processus protégés, en sélectionnant un de deux modes :

- **Terminer en cas d'exploit** : appliquez ce mode pour terminer le processus en cas de tentative d'exploitation d'une vulnérabilité.

En cas de détection d'une tentative d'exploitation d'une vulnérabilité dans un processus du système d'exploitation critique protégé, Kaspersky Security for Windows Server ne termine pas ce processus quel que soit le mode indiqué dans les paramètres du module Protection contre les exploits.

- **Informier uniquement** : appliquez ce mode pour recevoir des informations sur les instances d'exploits dans les processus protégés à l'aide des événements dans les journaux de sécurité.

Si ce mode est sélectionné, Kaspersky Security for Windows Server consigne toutes les tentatives d'exploitation des vulnérabilités en créant des événements.

## Administration de la Protection contre les exploits via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres du composant pour un seul ou pour l'ensemble des serveurs du réseau.

### Dans cette section

Navigation .....	<a href="#">537</a>
Configuration des paramètres de protection de la mémoire des processus .....	<a href="#">538</a>
Ajout d'un processus protégé .....	<a href="#">539</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

### Dans cette section

Accès aux paramètres de la stratégie pour la Protection contre les exploits.....	<a href="#">537</a>
Ouverture de la fenêtre des propriétés de la Protection contre les exploits.....	<a href="#">537</a>

## Accès aux paramètres de la stratégie pour la Protection contre les exploits

► *Pour accéder aux paramètres de protection contre les exploits via une stratégie de Kaspersky Security Center, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel du serveur**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Protection contre les exploits**.  
La fenêtre **Protection contre les exploits** s'ouvre.

Configurez la Protection contre les exploits en fonction des besoins.

## Ouverture de la fenêtre des propriétés de la Protection contre les exploits

► *Pour ouvrir la fenêtre **Propriétés : <nom du serveur>** de l'application pour la Protection contre les exploits, procédez comme suit :*

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <nom du serveur>** à l'aide d'une des méthodes suivantes :
  - Double-clic sur le nom du serveur protégé.
  - Sélectionnez l'option **Propriétés** dans le menu contextuel du serveur protégé.
 La fenêtre **Propriétés : <nom du serveur>** s'ouvre.

5. Dans la section **Applications**, sélectionnez **Kaspersky Security for Windows Server**.

6. Cliquez sur le bouton **Propriétés**.



La fenêtre **Configuration de Kaspersky Security for Windows Server** s'ouvre.

7. Sélectionnez la section **Protection en temps réel du serveur**.
8. Cliquez sur le bouton **Configuration** dans la sous-section **Protection contre les exploits**.

La fenêtre **Protection contre les exploits** s'ouvre.

Configurez la Protection contre les exploits en fonction des besoins.

## Configuration des paramètres de protection de la mémoire des processus

► *Pour configurer les paramètres de protection des Exploits pour les processus ajoutés à la liste des processus protégés, procédez comme suit :*

1. Ouvrez la fenêtre **Protection contre les exploits** (cf. section "**Accès aux paramètres de la stratégie pour la Protection contre les exploits**" à la page [537](#)).
2. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :

- **Empêcher l'exploit des processus vulnérables.**

Si la case est cochée, Kaspersky Security for Windows Server réduit les risques d'exploitation des vulnérabilités dans les processus dans la liste des processus protégés.

Si la case est décochée, Kaspersky Security for Windows Server ne protège pas les processus du serveur contre les exploits.

Cette case est décochée par défaut.

- **Terminer en cas d'exploit.**

Si ce mode est sélectionné, Kaspersky Security for Windows Server termine un processus protégé en cas de détection d'une tentative d'exploit si une technique de réduction de l'impact active a été appliquée au processus.

- **Informé uniquement.**

Si ce mode est sélectionné, Kaspersky Security for Windows Server signale les exploits en affichant la fenêtre de terminal à l'écran. Le processus exploité continue d'être exécuté.

Si lors du fonctionnement de l'application sous le mode **Terminer en cas d'exploit**, Kaspersky Security for Windows Server détecte un exploit dans un processus critique, le composant force le passage au mode **Informé uniquement**.

3. Configurez les paramètres suivants dans le groupe **Actions de prévention** :

- **Signaler les processus exploités via le service de terminal.**

Si la case est cochée, Kaspersky Security for Windows Server affiche à l'écran la fenêtre de terminal qui décrit le motif de déclenchement de la protection et indique le processus dans lequel la tentative d'exploitation de la vulnérabilité a été détectée.

Si la case est décochée, Kaspersky Security for Windows Server n'affiche pas à l'écran la fenêtre de terminal lors de la détection d'une tentative d'exploitation de la vulnérabilité ou d'achèvement du processus exploités. La fenêtre de terminal s'affiche quel que soit l'état

de fonctionnement du service Kaspersky Security Exploit Prevention. Cette case est cochée par défaut.

- **Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé.**

Si la case est cochée, Kaspersky Security for Windows Server réduit le risque d'exploitation de vulnérabilités des processus déjà lancés quel que soit l'état d'exécution du Service Kaspersky Security. Kaspersky Security for Windows Server ne protège pas les processus ajoutés après l'arrêt du Service Kaspersky Security. Une fois le service lancé, la réduction de l'impact de l'exploitation des vulnérabilités de tous les processus sera arrêtée.

Si la case est décochée, Kaspersky Security for Windows Server ne protège pas les processus contre l'exploitation des vulnérabilités quand le Service Kaspersky Security est arrêté.

Cette case est cochée par défaut.

4. Cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server enregistre les paramètres de protection de processus configurés et les applique.

## Ajout d'un processus protégé

Le composant Protection contre les exploits protège un certain nombre de processus par défaut. Vous pouvez exclure les processus de la zone de protection en décochant les cases correspondantes dans la liste.

► *Pour ajouter un processus à la liste des processus protégés :*

1. Ouvrez la fenêtre **Protection contre les exploits** (cf. section "**Accès aux paramètres de la stratégie pour la Protection contre les exploits**" à la page [537](#)).
2. Cliquez sur le bouton **Parcourir** sous l'onglet **Processus protégés**.  
La fenêtre standard de l'Explorateur Microsoft Windows s'ouvre.
3. Choisissez le processus que vous voulez ajouter à la liste.
4. Cliquez sur le bouton **Ouvrir**.  
Le nom du processus apparaît dans la ligne.
5. Cliquez sur **Ajouter**.  
Le processus indiqué est ajouté à la liste des processus protégés.
6. Sélectionnez le processus ajouté.
7. Cliquez sur **Définir les techniques de protection contre les exploits**.  
La fenêtre **Techniques de réduction de l'impact** s'ouvre.
8. Choisissez une des options d'application de la technique de réduction de l'impact :
  - **Appliquer toutes les techniques de protection contre les exploits disponibles.**  
Quand cette option a été sélectionnée, il est impossible de modifier la liste. Toutes les techniques disponibles pour un processus sont appliquées par défaut.
  - **Appliquer les techniques de protection contre les exploits indiquées.**

Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :

- a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.
- b. Cochez ou décochez la case **Appliquer la technique Attack Surface Reduction**.

9. Configurez les paramètres de la technique Attack Surface Reduction :

- Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
- Dans le champ **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :
  - Internet
  - Intranet local
  - Sites de confiance
  - Sites limités
  - Ordinateur

Ces paramètres sont applicables uniquement à Internet Explorer®.

10. Cliquez sur le bouton **OK**.

Le processus est ajouté à la zone de protection de la tâche.

## Administration de la Protection contre les exploits via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'un composant sur un serveur local.

### Dans cette section

Navigation .....	<a href="#">540</a>
Configuration des paramètres de protection de la mémoire des processus .....	<a href="#">541</a>
Ajout d'un processus protégé .....	<a href="#">542</a>

## Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface.

## Dans cette section

Accès aux paramètres généraux de la Protection contre les exploits .....	<a href="#">541</a>
Accès aux paramètres de protection du processus Protection contre les exploits .....	<a href="#">541</a>

## Accès aux paramètres généraux de la Protection contre les exploits

► Pour ouvrir la fenêtre **Paramètres de protection contre les exploits**, procédez comme suit :

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Security**.
2. Ouvrez le menu contextuel et sélectionnez l'option du menu **Protection contre les exploits : paramètres généraux**.

La fenêtre **Paramètres de protection contre les exploits** s'ouvre.

Configurez les paramètres généraux pour la Protection contre les exploits en fonction des besoins.

## Accès aux paramètres de protection du processus Protection contre les exploits

► Pour ouvrir la fenêtre **Paramètres de protection des processus**, procédez comme suit :

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Security**.
2. Ouvrez le menu contextuel et sélectionnez l'option de menu **Protection contre les exploits : paramètres de protection des processus**.

La fenêtre **Paramètres de protection des processus** s'ouvre.

Configurez les paramètres de protection du processus pour la Protection contre les exploits en fonction des besoins.

## Configuration des paramètres de protection de la mémoire des processus

► Pour ajouter un processus à la liste des processus protégés :

1. La fenêtre Paramètres de protection contre les exploits s'ouvre.
2. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :

- **Empêcher l'exploit des processus vulnérables.**

Si la case est cochée, Kaspersky Security for Windows Server réduit les risques d'exploitation des vulnérabilités dans les processus dans la liste des processus protégés.

Si la case est décochée, Kaspersky Security for Windows Server ne protège pas les processus du serveur contre les exploits.

Cette case est décochée par défaut.

- **Terminer en cas d'exploit.**

Si ce mode est sélectionné, Kaspersky Security for Windows Server termine un processus

protégé en cas de détection d'une tentative d'exploit si une technique de réduction de l'impact active a été appliquée au processus.

- **Informé uniquement.**

Si ce mode est sélectionné, Kaspersky Security for Windows Server signale les exploits en affichant la fenêtre de terminal à l'écran. Le processus exploité continue d'être exécuté.

Si lors du fonctionnement de l'application sous le mode **Terminer en cas d'exploit**, Kaspersky Security for Windows Server détecte un exploit dans un processus critique, le composant force le passage au mode **Informé uniquement**.

3. Configurez les paramètres suivants dans le groupe **Actions de prévention** :

- **Signaler les processus exploités via le service de terminal.**

Si la case est cochée, Kaspersky Security for Windows Server affiche à l'écran la fenêtre de terminal qui décrit le motif de déclenchement de la protection et indique le processus dans lequel la tentative d'exploitation de la vulnérabilité a été détectée.

Si la case est décochée, Kaspersky Security for Windows Server n'affiche pas à l'écran la fenêtre de terminal lors de la détection d'une tentative d'exploitation de la vulnérabilité ou d'achèvement du processus exploités. La fenêtre de terminal s'affiche quel que soit l'état de fonctionnement du service Kaspersky Security Exploit Prevention. Cette case est cochée par défaut.

- **Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé.**

Si la case est cochée, Kaspersky Security for Windows Server réduit le risque d'exploitation de vulnérabilités des processus déjà lancés quel que soit l'état d'exécution du Service Kaspersky Security. Kaspersky Security for Windows Server ne protège pas les processus ajoutés après l'arrêt du Service Kaspersky Security. Une fois le service lancé, la réduction de l'impact de l'exploitation des vulnérabilités de tous les processus sera arrêtée.

Si la case est décochée, Kaspersky Security for Windows Server ne protège pas les processus contre l'exploitation des vulnérabilités quand le Service Kaspersky Security est arrêté.

Cette case est cochée par défaut.

4. Dans la fenêtre **Paramètres de protection contre les exploits**, cliquez sur le bouton **OK**.

Kaspersky Security for Windows Server enregistre les paramètres de protection de processus configurés et les applique.

## Ajout d'un processus protégé

Le composant Protection contre les exploits protège un certain nombre de processus par défaut. Vous pouvez décocher les processus que vous ne souhaitez pas protéger dans la liste des processus protégés.

► *Pour ajouter un processus à la liste des processus protégés :*

1. Ouvrez la fenêtre Paramètres de protection des processus.
2. Pour ajouter des processus et les protéger contre l'intrusion de code malveillant ou réduire l'impact d'un exploit potentiel, procédez comme suit :

- a. Cliquez sur le bouton **Parcourir**.  
La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.
  - b. Dans la fenêtre qui s'ouvre, choisissez le processus que vous voulez ajouter à la liste.
  - c. Cliquez sur le bouton **Ouvrir**.
  - d. Cliquez sur **Ajouter**.  
Le processus indiqué est ajouté à la liste des processus protégés.
3. Sélectionnez le processus ajouté dans la liste.
  4. La configuration en cours apparaît sous l'onglet **Paramètres de protection du processus** :
    - **Nom du processus.**
    - **Exécution en cours.**
    - **Techniques de réduction de l'impact appliquées.**
    - **Paramètres de la technique Attack Surface Reduction.**
  5. Pour modifier les techniques de protection contre les exploits appliquées au processus, sélectionnez l'onglet **Techniques de réduction de l'impact**.
  6. Choisissez une des options d'application de la technique de réduction de l'impact :
    - **Appliquer toutes les techniques de protection contre les exploits disponibles.**  
Quand cette option a été sélectionnée, il est impossible de modifier la liste. Toutes les techniques disponibles pour un processus sont appliquées par défaut.
    - **Appliquer les techniques indiquées de protection contre les exploits pour le processus.**  
Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :
      - a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.
  7. Configurez les paramètres de la technique Attack Surface Reduction :
    - Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
    - Dans le champ **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :
      - Internet
      - Intranet local
      - Sites de confiance
      - Sites limités
      - Ordinateur
- Ces paramètres sont applicables uniquement à Internet Explorer®.
8. Cliquez sur le bouton **OK**.  
Le processus est ajouté à la zone de protection de la tâche.

## Techniques de protection contre les exploits

Tableau 71. Techniques de protection contre les exploits

Technique de protection contre les exploits	Description
Data Execution Prevention (DEP)	Prévention de l'exécution des données, à savoir l'interdiction de l'exécution d'un code aléatoire dans un secteur protégé de la mémoire.
Address Space Layout Randomization (ASLR)	Modification de la disposition des structures de données dans l'espace d'adresse du processus.
Structured Exception Handler Overwrite Protection (SEHOP)	Substitution de l'enregistrement dans la structure des exclusions ou substitution du processeur d'exclusions.
Null Page Allocation	Prévention de la réorientation de l'index nul.
LoadLibrary Network Call Check (Anti ROP)	Protection contre le chargement des bibliothèques dynamiques depuis les chemins de réseau.
Executable Stack (Anti ROP)	Interdiction de l'exécution non autorisée des zones de la pile.
Anti RET Check (Anti ROP)	Contrôle de l'invocation sûre d'une fonction via l'instruction CALL.
Anti Stack Pivoting (Anti ROP)	Protection contre le déplacement de l'index de pile ESP vers l'adresse exploitée.
Simple Export Adress Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection de l'accès en lecture du tableau d'exportation des adresses (Export Address Table) pour les modules kernel32.dll, kernelbase.dll et ntdll.dll
Heap Spray Allocation (Heapspray)	Protection contre l'attribution de mémoire en cas d'exécution d'un code malveillant.
Execution Flow Simulation (Anti Return Oriented Programming)	Détection de chaînes d'instructions suspectes (gadget ROP possible) dans le composant Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection contre l'élévation de privilèges via une vulnérabilité dans le pilote AFD (exécution du code arbitraire sur le cercle nul dans l'appel QueryIntervalProfile).
Attack Surface Reduction (ASR)	Interdiction du lancement de modules vulnérables via le processus protégé.
Anti Process Hollowing (Hollowing)	Protection contre la création et l'exécution des copies malveillantes des processus bloqués.
Anti AtomBombing (APC)	Exploit global atom table via des appels APC.
Anti CreateRemoteThread (RThreadLocal)	Un autre processus a créé une thread dans un processus protégé.
Anti CreateRemoteThread (RThreadRemote)	Un autre processus a créé une thread de contrôle dans un processus protégé.

# Administration du stockage hiérarchique

Cette section contient des informations sur l'analyse antivirus des fichiers qui se trouvent dans des stockages hiérarchiques et dans des systèmes de sauvegarde.

## Contenu du chapitre

A propos du stockage hiérarchique .....	<a href="#">545</a>
Configuration des paramètres du système HSM via le plug-in d'administration .....	<a href="#">546</a>
Configuration des paramètres du système HSM via la Console de l'application .....	<a href="#">547</a>

## A propos du stockage hiérarchique

La gestion du stockage hiérarchique (ci-après système HSM) permet de transférer des données entre des disques locaux rapides et des périphériques lents de stockage d'informations de longue durée. Malgré les avantages évidents des périphériques de rappel rapides, leur utilisation reste chère pour la majorité des entreprises. Les systèmes HSM garantissent le transfert des informations non utilisées vers des périphériques bon marché de stockage à distance, ce qui réduit les dépenses de la société.

Les systèmes HSM enregistrent une partie des informations dans des référentiels distants et les restaure en cas de besoin. Les systèmes HSM assurent un contrôle permanent de l'utilisation des fichiers et définissent ceux qui peuvent être déplacés dans le stockage distant et ceux qu'il est préférable de laisser sur les périphériques de stockage local. Les fichiers sont déplacés vers le stockage distant s'ils ne sont pas sollicités pendant une période définie. Si l'utilisateur sollicite le fichier situé dans le stockage distant, celui est transféré à nouveau vers le disque local. Ce principe garantit à l'utilisateur un accès rapide à un volume important d'informations qui est bien supérieur à la capacité du disque.

Lors du déplacement d'un fichier depuis le disque local vers le stockage distant, le système HSM conserve le lien vers l'emplacement effectif de ce fichier. En cas de sollicitation d'un fichier contenant un lien, le système définit l'emplacement des données sur le périphérique de sauvegarde. Le remplacement des fichiers par des liens dans l'emplacement de stockage permet d'obtenir un stockage à la capacité quasiment illimitée.

Certains systèmes HSM permettent de conserver une partie des fichiers dans le stockage local. Dans ce cas, une grande partie du fichier est déplacée vers le stockage distant tandis qu'une petite partie du fichier source reste sur le stockage local.

Les systèmes HSM proposent deux méthodes d'accès aux informations situées dans le stockage hiérarchique :

- Points d'analyse.
- Attributs étendus du fichier.



## Configuration des paramètres du système HSM via le plug-in d'administration

Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut inchangée pour le paramètre de type d'accès au stockage hiérarchique (système non HSM).

Pour configurer l'accès au stockage hiérarchique, vous devez indiquer la manière dont le système HSM détermine l'emplacement du fichier analysé. Ces informations figurent dans la documentation du système HSM utilisé.

► Pour définir le type d'accès pour le stockage hiérarchique, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans l'arborescence de la console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Paramètres de l'application**.
6. Dans la sous-section **Montée en puissance et interface**, cliquez sur le bouton **Configuration**.  
La fenêtre **Paramètres avancés de l'application** s'ouvre.
7. Ouvrez le lien **Stockage hiérarchique**.
8. Sélectionnez l'option d'accès au système HSM :

- **Aucun système HSM.**

Kaspersky Security for Windows Server n'utilise pas les paramètres du système HSM lors de l'exécution des tâches d'analyse à la demande.

Cette option est sélectionnée par défaut.

- **Le système HSM utilise des points d'analyse.**

Kaspersky Security for Windows Server utilise des points de traitement réitéré pour l'analyse des fichiers dans le stockage distant lors de l'exécution des tâches d'analyse à la demande.

- **Le système HSM utilise les attributs élargis du fichier.**

Kaspersky Security for Windows Server exploite des attributs de fichier étendus pour analyser les fichiers dans le stockage distant lors de l'exécution de la tâche Analyse à la demande.

- **Système HSM non identifié.**

Kaspersky Security for Windows Server analyse tous les fichiers comme les fichiers situés dans un stockage distant, lors de l'exécution des tâches d'analyse à la demande.

Il est déconseillé d'utiliser cette option.

Si vous indiquez la mauvaise version ou sélectionnez l'option **Système HSM non identifié**, Kaspersky Security for Windows Server risque de déterminer incorrectement l'emplacement des objets, ce qui augmentera leur temps de traitement.

9. Cliquez sur le bouton **OK**.

Les paramètres du système HSM définis seront enregistrés.

## Configuration des paramètres du système HSM via la Console de l'application

Si vous n'utilisez pas de systèmes HSM, laissez la valeur par défaut inchangée pour le paramètre de type d'accès au stockage hiérarchique (système non HSM).

Pour configurer l'accès au stockage hiérarchique, vous devez indiquer la manière dont le système HSM détermine l'emplacement du fichier analysé. Ces informations figurent dans la documentation du système HSM utilisé.

► Pour définir le type d'accès pour le stockage hiérarchique, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Security**.
2. Sélectionnez l'option **Stockage hiérarchique**.

La fenêtre **Paramètres du système HSM** s'ouvre

3. Sous l'onglet **Stockage hiérarchique**, définissez les paramètres du système HSM :

- **Aucun système HSM.**

Kaspersky Security for Windows Server n'utilise pas les paramètres du système HSM lors de l'exécution des tâches d'analyse à la demande.

Cette option est sélectionnée par défaut.

- **Le système HSM utilise des points d'analyse.**

Kaspersky Security for Windows Server utilise des points de traitement réitéré pour l'analyse des fichiers dans le stockage distant lors de l'exécution des tâches d'analyse à la demande.

- **Le système HSM utilise les attributs élargis du fichier.**

Kaspersky Security for Windows Server exploite des attributs de fichier étendus pour analyser les fichiers dans le stockage distant lors de l'exécution de la tâche Analyse à la

demande.

- **Système HSM non identifié.**

Kaspersky Security for Windows Server analyse tous les fichiers comme les fichiers situés dans un stockage distant, lors de l'exécution des tâches d'analyse à la demande.

Il est déconseillé d'utiliser cette option.

Si vous indiquez la mauvaise version ou sélectionnez l'option **Système HSM non identifié**, Kaspersky Security for Windows Server risque de déterminer incorrectement l'emplacement des objets, ce qui augmentera leur temps de traitement.

4. Cliquez sur le bouton **OK**.

Les paramètres du système HSM définis seront enregistrés.

# Intégration aux systèmes tiers

Cette section décrit l'intégration de Kaspersky Security for Windows Server aux fonctions et technologies tierces.

## Contenu du chapitre

Contrôle des performances. Compteurs de Kaspersky Security for Windows Server .....	<a href="#">549</a>
Intégration à WMI .....	<a href="#">565</a>

## Contrôle des performances. Compteurs de Kaspersky Security for Windows Server

La présente section fournit des informations sur les compteurs Kaspersky Security for Windows Server : Compteurs de performance, de Moniteur système et compteurs et interruptions SNMP.

### Dans cette section

Compteurs de performance pour l'application Moniteur système .....	<a href="#">549</a>
Compteurs et interruptions SNMP de Kaspersky Security for Windows Server .....	<a href="#">556</a>

## Compteurs de performance pour l'application Moniteur système

Cette section fournit des informations sur les compteurs de performance pour l'application Moniteur Système de Microsoft Windows enregistrés par Kaspersky Security for Windows Server pendant l'installation.

### Dans cette section

A propos des compteurs SNMP de Kaspersky Security for Windows Server .....	<a href="#">550</a>
Total de requêtes rejetées .....	<a href="#">550</a>
Total de requêtes ignorées .....	<a href="#">552</a>
Nombre de requêtes non traitées en raison d'un manque de ressources système .....	<a href="#">552</a>
Nombre de requêtes envoyées pour traitement .....	<a href="#">553</a>
Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers .....	<a href="#">553</a>
Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers .....	<a href="#">554</a>
Nombre d'éléments dans la file d'attente des objets infectés .....	<a href="#">554</a>
Nombre d'objets traités par seconde .....	<a href="#">555</a>

## A propos des compteurs SNMP de Kaspersky Security for Windows Server

Les composants à installer de Kaspersky Security for Windows Server incluent par défaut le composant **Compteurs de performance**. Pendant l'installation, Kaspersky Security for Windows Server enregistre ses compteurs de performance pour l'application Moniteur système de Microsoft Windows.

Grâce aux compteurs de Kaspersky Security for Windows Server, vous pouvez contrôler les performances de l'application 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 Security for Windows Server et les échecs de fonctionnement.

Pour consulter les compteurs de performance de Kaspersky Security for Windows Server, ouvrez la console **Optimisation** dans l'élément **Administration** du panneau de configuration de Windows.

Les sections suivantes abordent la définition des compteurs, les intervalles de calcul des relevés recommandés, les seuils et les recommandations pour la configuration de Kaspersky Security for Windows Server lorsque les compteurs dépassent ces valeurs.

### Total de requêtes rejetées

Tableau 72. Total de requêtes rejetées

<b>Nom</b>	Total de requêtes rejetées (Total number of requests denied)
<b>Définition</b>	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de l'application, le calcul est réalisé depuis la dernière exécution de Kaspersky Security for Windows Server. L'application ignore les objets dont les requêtes de traitement sont rejetées par les processus de Kaspersky Security for Windows Server.
<b>Fonction</b>	Ce compteur permet d'identifier : <ul style="list-style-type: none"> <li>• La réduction de la qualité de la Protection en temps réel en raison d'une charge complète des processus de Kaspersky Security for Windows Server.</li> <li>• L'interruption de la Protection en temps réel en raison d'un refus du gestionnaire d'intercepteurs de fichiers.</li> </ul>
<b>Valeur normale / seuil</b>	0 / 1
<b>Intervalle de calcul des relevés recommandé</b>	1 heure

<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés.</p> <p>Les situations suivantes sont envisageables en fonction du "comportement" du compteur :</p> <ul style="list-style-type: none"><li>• le compteur indique certains plusieurs requêtes rejetées durant une longue période : tous les processus de Kaspersky Security for Windows Server étaient totalement occupés, si bien que Kaspersky Security for Windows Server n'a pas pu analyser les objets.</li></ul> <p>Pour éviter que des objets soient ignorés, augmentez le nombre de processus de l'application pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security for Windows Server <b>Quantité maximale de processus actifs</b> et <b>Nombre de processus de protection en temps réel</b>.</p> <ul style="list-style-type: none"><li>• Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : le gestionnaire d'intercepteurs de fichiers ne fonctionne plus. Kaspersky Security for Windows Server n'analyse pas les objets à l'accès. Relancez Kaspersky Security for Windows Server.</li></ul>
---	---

## Total de requêtes ignorées

Tableau 73. Total de requêtes ignorées

<b>Nom</b>	Total de requêtes ignorées (Total number of requests skipped).
<b>Définition</b>	<p>Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par Kaspersky Security for Windows Server mais qui n'ont pas donné d'événement sur la fin du traitement, ce nombre est calculé depuis la dernière exécution de l'application.</p> <p>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 <b>Total des requêtes ignorées</b> augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a reçu la requête de traitement (ils étaient occupés) ou n'a pas envoyé d'événement sur la fin du traitement, Kaspersky Security for Windows Server ignore cet objet et la valeur du compteur <b>Total des requêtes rejetées</b> augmente d'une unité.</p>
<b>Fonction</b>	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
<b>Valeur normale / seuil</b>	0 / 1.
<b>Intervalle de calcul des relevés recommandé</b>	1 heure
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>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.</p> <p>Si la vitesse d'analyse n'est pas satisfaisante, redémarrez Kaspersky Security for Windows Server afin de rétablir les flux gelés.</p>

## Nombre de requêtes non traitées en raison d'un manque de ressources système

Tableau 74. Nombre de requêtes non traitées en raison d'un manque de ressources système

<b>Nom</b>	Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)
<b>Définition</b>	<p>Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources système (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Security for Windows Server.</p> <p>Kaspersky Security for Windows Server ignore les objets dont les requêtes de traitement ne sont pas traitées par le pilote d'interception de fichiers.</p>
<b>Fonction</b>	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.
<b>Valeur normale / seuil</b>	0 / 1

<b>Intervalle de calcul des relevés recommandé</b>	1 heure
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	Si le compteur affiche une valeur différente de zéro, les processus de travail de Kaspersky Security for Windows Server 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.

## Nombre de requêtes envoyées pour traitement

Tableau 75. Nombre de requêtes envoyées pour traitement

<b>Nom</b>	Nombre de requêtes envoyées pour traitement.
<b>Définition</b>	Nombre d'objets en attente de traitement par les processus actifs.
<b>Fonction</b>	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Security for Windows Server et le niveau général de l'activité de fichiers sur le serveur.
<b>Valeur normale / seuil</b>	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur le serveur.
<b>Intervalle de calcul des relevés recommandé</b>	Une minute
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	non

## Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Tableau 76. Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

<b>Nom</b>	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers.
<b>Définition</b>	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)
<b>Fonction</b>	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 Security for Windows Server et d'y remédier.
<b>Valeur normale / seuil</b>	Varie/40.



<b>Intervalle de calcul des relevés recommandé</b>	Une minute
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>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 Security for Windows Server ignorera l'objet.</p> <p>Augmentez le nombre de processus de Kaspersky Security for Windows Server pour les tâches de protection en temps réel. Vous pouvez utiliser les paramètres de Kaspersky Security for Windows Server <b>Quantité maximale de processus actifs</b> et <b>Nombre de processus de protection en temps réel</b>.</p>

## Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Tableau 77. Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

<b>Nom</b>	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers
<b>Définition</b>	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).
<b>Fonction</b>	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
<b>Valeur normale / seuil</b>	Varie/40.
<b>Intervalle de calcul des relevés recommandé</b>	Une minute
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>Si la valeur de ce compteur dépasse en permanence et de beaucoup la valeur du compteur <b>Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers</b>, Kaspersky Security for Windows Server répartit de manière inégale la charge sur les processus exécutés.</p> <p>Relancez Kaspersky Security for Windows Server.</p>

## Nombre d'éléments dans la file d'attente des objets infectés

Tableau 78. Nombre d'éléments dans la file d'attente des objets infectés

<b>Nom</b>	Nombre d'éléments dans la file d'attente des objets infectés (Number of items in the infected object queue).
<b>Définition</b>	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment.

<b>Fonction</b>	<p>Ce compteur permet d'identifier :</p> <ul style="list-style-type: none"> <li>• L'interruption de la Protection en temps réel en raison d'un éventuel refus du gestionnaire d'intercepteurs de fichiers.</li> <li>• La surcharge des processus suite à une répartition inégale du temps de processeur entre Kaspersky Security for Windows Server et les autres applications exécutées.</li> <li>• Les épidémies de virus.</li> </ul>
<b>Valeur normale / seuil</b>	<p>La valeur du compteur peut être différente de zéro tant que Kaspersky Security for Windows Server traite les objets probablement infectés ou infectés découverts mais elle revient sur zéro juste après le traitement / La valeur du compteur est différente de zéro pendant une longue période.</p>
<b>Intervalle de calcul des relevés recommandé</b>	<p>Une minute</p>
<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>Si la valeur du compteur n'est pas égale à zéro pendant une longue période :</p> <ul style="list-style-type: none"> <li>• Kaspersky Security for Windows Server ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Relancez Kaspersky Security for Windows Server.</li> <li>• Manque de temps de processus pour le traitement des objets ; Accordez à Kaspersky Security for Windows Server plus de temps de processeur, par exemple en réduisant la charge des autres applications sur le serveur.</li> <li>• Une épidémie de virus s'est déclenchée.</li> </ul> <p>L'émergence d'une épidémie de virus est également indiquée par le nombre élevé d'objets infectés ou probablement infectés découverts dans la tâche Protection des fichiers en temps réel. Les informations relatives au nombre d'objets détectés figure dans les statistiques de la tâche ou dans le journal d'exécution de la tâche.</p>

## Nombre d'objets traités par seconde

Tableau 79. Nombre d'objets traités par seconde

<b>Nom</b>	<p>Nombre d'objets traités par seconde.</p>
<b>Définition</b>	<p>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</p>
<b>Fonction</b>	<p>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 Security for Windows Server ou d'un échec de Kaspersky Security for Windows Server et d'y remédier.</p>
<b>Valeur normale / seuil</b>	<p>Varie / non.</p>
<b>Intervalle de calcul des relevés recommandé</b>	<p>Une minute</p>

<b>Recommandation pour la configuration si la valeur dépasse la valeur limite</b>	<p>Les valeurs du compteur dépendent des paramètres de Kaspersky Security for Windows Server et de la charge des processus des autres applications sur le serveur.</p> <p>Observez le niveau moyen du compteur au cours d'une longue période. Si le niveau du compteur a diminué, c'est peut-être à cause d'une des situations suivantes :</p> <ul style="list-style-type: none"> <li>• Les processus de travail de Kaspersky Security for Windows Server ne disposent pas des ressources de processeur suffisantes pour traiter les objets. Accordez à Kaspersky Security for Windows Server plus de temps de processeur, par exemple en réduisant la charge des autres applications sur le serveur.</li> <li>• Un échec s'est produit dans le fonctionnement de Kaspersky Security for Windows Server (plusieurs flux sont gelés). Relancez Kaspersky Security for Windows Server.</li> </ul>
---	---

## Compteurs et interruptions SNMP de Kaspersky Security for Windows Server

Cette section contient des informations sur les compteurs et les interruptions SNMP de Kaspersky Security for Windows Server.

### Dans cette section

A propos des compteurs et interruptions SNMP de Kaspersky Security for Windows Server.....	<a href="#">556</a>
Compteurs SNMP de Kaspersky Security for Windows Server .....	<a href="#">556</a>
Interruptions SNMP de Kaspersky Security for Windows Server .....	<a href="#">559</a>

### A propos des compteurs et interruptions SNMP de Kaspersky Security for Windows Server

Si vous avez inclus le composant Compteurs et pièges SNMP dans les composants antivirus à installer, vous pouvez consulter les compteurs et les interruptions de Kaspersky Security for Windows Server à l'aide du protocole Simple Network Management Protocol (SNMP).

Pour consulter les compteurs et les interruptions de Kaspersky Security for Windows Server depuis le poste de travail de l'administrateur, lancez sur le serveur protégé le service SNMP (SNMP Service) et le service d'interruptions SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

### Compteurs SNMP de Kaspersky Security for Windows Server

Cette section propose un tableau contenant la description des paramètres des compteurs SNMP de Kaspersky Security for Windows Server.

## Dans cette section

Compteurs de performance .....	<a href="#">557</a>
Compteurs de quarantaine .....	<a href="#">557</a>
Compteurs de sauvegarde .....	<a href="#">557</a>
Compteurs généraux .....	<a href="#">558</a>
Compteur de mise à jour .....	<a href="#">558</a>
Compteurs de Protection en temps réel .....	<a href="#">558</a>

## Compteurs de performance

Tableau 80. Compteurs de performance

Compteur	Définition
currentRequestsAmount	Nombre de requêtes envoyées pour traitement(cf. page <a href="#">553</a> )
currentInfectedQueueLength	Nombre d'éléments dans la file d'attente d'objets infectés (cf. section "Nombre d'éléments dans la file d'attente des objets infectés" à la page <a href="#">554</a> )
currentObjectProcessingRate	Nombre d'objets traités par seconde (à la page <a href="#">555</a> )
currentWorkProcessesNumber	Nombre actuel de processus actifs utilisés par Kaspersky Security for Windows Server

## Compteurs de quarantaine

Tableau 81. Compteurs de quarantaine

Compteur	Définition
totalObjects	Nombre d'objets présents actuellement en quarantaine
totalSuspiciousObjects	Nombre d'objets probablement infectés présents actuellement en quarantaine
currentStorageSize	Volume de données en quarantaine (Mo)

## Compteurs de sauvegarde

Tableau 82. Compteurs de sauvegarde

Compteur	Définition
currentBackupStorageSize	Volume de données en sauvegarde (Mo)

## Compteurs généraux

Tableau 83. Compteurs généraux

Compteur	Définition
lastCriticalAreasScanAge	Période écoulée depuis la dernière analyse rapide du serveur (intervalle de temps en secondes entre la date de fin de la tâche portant le statut <i>Tâche d'analyse rapide</i> et le moment actuel).
licenseExpirationDate	Date d'expiration de la licence Si des clés active et additionnelle ou des codes d'activation ont été ajoutés, la date affichée est la date d'échéance de la licence associée à la clé additionnelle ou au code d'activation.
currentApplicationUptime	Durée de fonctionnement de Kaspersky Security for Windows Server depuis sa dernière exécution (en centièmes de secondes).
currentFileMonitorTaskStatus	Etat de la tâche Protection des fichiers en temps réel : <b>On</b> – en cours d'exécution ; <b>Off</b> – arrêtée ou mise en pause.

## Compteur de mise à jour

Tableau 84. Compteur de mises à jour

Compteur	Définition
avBasesAge	"Age" des bases (intervalle de temps en centièmes de seconde entre la date de création des dernières mises à jour installées et l'heure actuelle).

## Compteurs de Protection en temps réel

Tableau 85. Compteurs de Protection en temps réel

Compteur	Définition
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalInfectedObjectsFound	Nombre d'objets infectés et autres découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalSuspiciousObjectsFound	Nombre d'objets probablement infectés découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalVirusesFound	Nombre d'objets détectés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsQuarantined	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Security for Windows Server a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotQuarantined	Nombre total d'objets infectés ou probablement infectés que Kaspersky Security for Windows Server a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

Compteur	Définition
totalObjectsDisinfected	Nombre total d'objets infectés qui ont été désinfectés par Kaspersky Security for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDisinfected	Nombre total d'objets infectés ou autres que Kaspersky Security for Windows Server a tenté de désinfecter en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsDeleted	Nombre total d'objets infectés, probablement infectés ou autres désinfectés par Kaspersky Security for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDeleted	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Security for Windows Server a tenté de désinfecter en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsBackedUp	Nombre total d'objets infectés ou autres placés dans la Sauvegarde par Kaspersky Security for Windows Server ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotBackedUp	Nombre total d'objets infectés ou autres que Kaspersky Security for Windows Server a tenté de placer en vain dans la Sauvegarde ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

## Interruptions SNMP de Kaspersky Security for Windows Server

Les options des interruptions SNMP de Kaspersky Security for Windows Server sont résumées comme suit :

- eventThreatDetected : un objet a été détecté.  
Les options d'interruptions sont les suivantes :
  - eventDateAndTime
  - eventSeverity
  - computerName
  - UserName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds : dépassement de la taille maximale de la Sauvegarde. Le volume total de données de la Sauvegarde dépasse la valeur du paramètre **Taille maximale de sauvegarde (Mo)**. Kaspersky Security for Windows Server poursuit la mise en sauvegarde des objets infectés.

Les options d'interruptions sont les suivantes :

- eventDateAndTime
- eventSeverity
- eventSource
- eventThresholdBackupStorageSizeExceeds : Le seuil d'espace libre pour la sauvegarde est atteint. La quantité d'espace disponible dans la sauvegarde, définie par le paramètre **Seuil d'espace disponible (Mo)**, est inférieure ou égale à la valeur indiquée. Kaspersky Security for Windows Server poursuit la mise en sauvegarde des objets infectés.

Les options d'interruptions sont les suivantes :

- eventDateAndTime
- eventSeverity
- eventSource
- eventQuarantineStorageSizeExceeds : dépassement de la taille maximum de la quarantaine. Le volume total de données de la quarantaine a dépassé la valeur du paramètre **Taille maximale de la quarantaine (Mo)**. Kaspersky Security for Windows Server poursuit la mise en quarantaine des objets probablement infectés.

Les options d'interruptions sont les suivantes :

- eventDateAndTime
- eventSeverity
- eventSource
- eventObjectNotQuarantined : erreur de quarantaine.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- UserName
- computerName
- objectName
- storageObjectNotAddedEventReason
- eventObjectNotBackuper : erreur d'enregistrement d'une copie de l'objet dans la Sauvegarde.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- objectName
- UserName
- computerName

- storageObjectNotAddedEventReason
- eventQuarantineInternalError : erreur de quarantaine interne.  
Les options d'interruptions sont les suivantes :
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError : erreur de sauvegarde.  
Les options d'interruptions sont les suivantes :
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated : la base antivirus n'est plus à jour. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de l'application (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).  
Les options d'interruptions sont les suivantes :
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated : la base antivirus est périmée. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de l'application (tâche locale, tâche de groupe ou tâche pour les sélections d'ordinateurs).  
Les options d'interruptions sont les suivantes :
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted : Kaspersky Security for Windows Server est en cours d'exécution.  
Les options d'interruptions sont les suivantes :
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown : Kaspersky Security for Windows Server est arrêté.  
Les options d'interruptions sont les suivantes :



- eventSeverity
- eventDateAndTime
- eventSource
- eventCriticalAreasScanWasntPerformForALongTime : analyse des zones critiques non réalisée depuis longtemps. Le nombre de jours écoulés depuis la dernière exécution de la tâche d'analyse des zones critiques est compté.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- days
- eventLicenseHasExpired : licence expirée.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- eventLicenseExpiresSoon : la durée de validité de la licence arrive bientôt à échéance. Le nombre de jour restant avant la fin de la validité de la licence est compté

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- days
- eventTaskInternalError : erreur d'exécution de la tâche.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource
- errorCode
- knowledgeBaselId
- taskName
- eventUpdateError : erreur de performances de la tâche de mise à jour.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- taskName

- updaterErrorEventReason

Descriptions des options d'interruption et valeurs possibles des paramètres :

- eventDateAndTime : date et heure de l'événement.
- eventSeverity : niveau d'importance.

L'option peut prendre les valeurs suivantes :

- critical (1) – critique,
- warning (2) – avertissement,
- info (3) – informations.
- userName : un nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté).
- computerName : nom du serveur (par exemple, nom du serveur dont l'utilisateur a tenté d'accéder à un fichier infecté).
- eventSource : composant fonctionnel pendant le fonctionnement duquel l'événement s'est produit.

L'option peut prendre les valeurs suivantes :

- unknown (0) – composant fonctionnel non identifié ;
- quarantine (1) – Quarantaine ;
- backup (2) – Sauvegarde ;
- reporting (3) – Journaux d'exécution de la tâche ;
- updates (4) – Mise à jour ;
- realTimeProtection (5) – Protection des fichiers 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 Security for Windows Server dans son ensemble ;
- systemAudit (8) – Journal d'audit système.
- eventReason : déclencheur de l'événement : cause de l'événement.

L'option peut prendre les valeurs suivantes :

- 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 (privileges d'accès insuffisants ou le chemin de réseau indiqué dans les paramètres de la quarantaine est incorrect). Dans ce cas, Kaspersky Security for Windows Server utilise le dossier de sauvegarde ou de quarantaine indiqué par défaut.
- objectName : nom de l'objet (par exemple, nom du fichier contenant le virus)
- threatName : Nom de l'objet détecté selon la classification de l'Encyclopédie des virus (<https://encyclopedia.kaspersky.com/knowledge/classification/>). Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Security for Windows Server renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet d'un objet détecté dans le journal d'exécution de la tâche (cf. section "Configuration des paramètres du journal" à la page [109](#)).

- detectType : type d'objet détecté.

L'option peut prendre les valeurs suivantes :

- undefined (0) – indéterminé ;
  - virware – virus et vers de réseau traditionnels ;
  - trojware – chevaux de Troie ;
  - malware – autres applications malveillantes ;
  - adware – applications publicitaires ;
  - pornware – logiciels pornographiques ;
  - riskware – applications légitimes pouvant être utilisées à des fins malveillantes pour endommager l'ordinateur ou les données personnelles de l'utilisateur.
- detectCertainty : coefficient de certitude pour la détection d'une menace.

L'option peut prendre les valeurs suivantes :

- Suspicion (probablement infecté) : Kaspersky Security for Windows Server a détecté une correspondance partielle entre un morceau de code de l'objet et un morceau de code malveillant connu.
  - Sure (infecté) : Kaspersky Security for Windows Server a détecté une équivalence parfaite entre une partie du code de l'objet et une partie d'un code malveillant connu.
- days : nombre de jours (par exemple, nombre de jours d'ici la fin de la validité de la licence).
  - errorCode : un code d'erreur.
  - knowledgeBaselId : adresse de l'article dans la banque de solutions (par exemple, adresse de l'article décrivant une erreur quelconque).
  - taskName : un nom de tâche.
  - updaterErrorEventReason : cause de la non-application de la mise à jour.

L'option peut prendre les valeurs suivantes :

- reasonUnknown(0) – cause indéterminée ;
- reasonAccessDenied – accès interdit ;
- reasonUrlsExhausted – fin de la liste des sources de mise à jour ;
- reasonInvalidConfig – fichier de configuration incorrect ;
- reasonInvalidSignature – signature invalide ;
- reasonCantCreateFolder – création du répertoire impossible ;
- reasonFileOperError – erreur de fichier ;
- reasonDataCorrupted – objet corrompu ;
- reasonConnectionReset – arrêt de la connexion ;
- reasonTimeOut – délai d'attente pour la connexion expiré ;
- reasonProxyAuthError – erreur d'authentification sur le serveur proxy ;
- reasonServerAuthError – erreur d'authentification sur le serveur ;
- reasonHostNotFound – ordinateur introuvable ;

- reasonServerBusy – serveur inaccessible ;
- reasonConnectionError – erreur de connexion ;
- reasonModuleNotFound – objet introuvable ;
- reasonBlstCheckFailed(16) – erreur de vérification de la liste noire des clés. Il se peut qu'une actualisation ait été diffusée au moment de la mise à jour des bases de données. Essayez à nouveau de réaliser la mise à jour dans quelques minutes.
- storageObjectNotAddedEventReason : cause du non placement de l'objet en sauvegarde ou en quarantaine.

L'option peut prendre les valeurs suivantes :

- reasonUnknown(0) – cause indéterminée ;
- reasonStorageInternalError : erreur ; Kaspersky Security for Windows Server doit être restauré.
- reasonStorageReadOnly : la base de données est en lecture seule ; Kaspersky Security for Windows Server doit être restauré.
- reasonStorageIOError : erreur entrée/sortie : a) Kaspersky Security for Windows Server est endommagé, Kaspersky Security for Windows Server doit être restauré ; b) le disque contenant les fichiers de Kaspersky Security for Windows Server est endommagé.
- reasonStorageCorrupted : le stockage est endommagé ; Kaspersky Security for Windows Server doit être restauré.
- reasonStorageFull – la base de données est remplie ; veuillez faire de la place sur le disque.
- reasonStorageOpenError : impossible d'ouvrir le fichier base de données ; Kaspersky Security for Windows Server doit être restauré.
- reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigences de Kaspersky Security for Windows Server.
- reasonObjectNotFound – l'objet placé dans la Quarantaine n'existe pas sur le disque.
- reasonObjectAccessError – privilèges 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.

## Intégration à WMI

Kaspersky Security for Windows Server prend en charge l'intégration à l'infrastructure de gestion Windows (WMI) : vous pouvez utiliser les systèmes clients qui emploient WMI pour recevoir les données via le standard Web-Based Enterprise Management (WBEM) afin d'obtenir des informations sur l'état de Kaspersky Security for Windows Server et de ses composants.

Une fois installé, Kaspersky Security for Windows Server enregistre un module exclusif dans le système afin de simplifier la création d'un espace de noms Kaspersky Security for Windows Server l'espace de noms racine WMI sur l'ordinateur local. Un espace de noms Kaspersky Security for Windows Server vous permet d'utiliser des catégories et des instances Kaspersky Security for Windows Server et leurs propriétés.

Les valeurs de certaines propriétés d'instance dépendent des types de tâche.

Une *tâche non périodique* est une tâche d'application qui n'est pas limitée dans le temps et qui peut être en exécution constante ou arrêtée. Il n'existe pas d'état d'avancement pour ce genre de tâche. Les résultats de l'exécution de la tâche sont enregistrés en continu pendant l'exécution de la tâche en tant qu'événements uniques (par exemple, détection d'un objet infecté par une des tâches de Protection en temps réel du serveur). Ce type de tâche est administré via les stratégies de Kaspersky Security Center.

Une *tâche périodique* est une tâche d'application qui est limitée dans le temps et dont l'état d'avancement est affiché en pour cent. Les résultats de la tâche sont générés quand la tâche est complétée et sont représentés en tant qu'élément unique ou qu'état modifié de l'application (par exemple, mise à jour des bases de l'application terminée, fichiers de configuration créés pour les tâches de création de règles). Un nombre de tâches périodiques du même type peuvent être exécutées simultanément sur un seul ordinateur (trois tâches d'analyse à la demande avec différentes zones d'analyse). Les tâches périodiques peuvent être administrées via Kaspersky Security Center en tant que tâches de groupe.

Si vous créez les requêtes d'espace de noms WMI à l'aide d'outils et si vous recevez les données dynamiques depuis les espaces de noms WMI sur votre réseau d'entreprise, vous pourrez obtenir les informations relatives à l'état actuel de l'application (cf. tableau ci-dessous).

Tableau 86. Informations sur l'état de l'application

Propriété de l'instance	Description	Valeurs
ProductName	Le nom de l'application installée.	Nom complet de l'application sans le numéro de version.
ProductVersion	La version complète de l'application installée.	Numéro de version de l'application complet, avec le numéro de build.
InstalledPatches	L'ensemble des noms affichés des correctifs déployés pour l'application.	Liste des correctifs critiques installés pour l'application.
IsLicenseInstalled	L'état d'activation de l'application.	Etat de la clé utilisée pour activer l'application. Valeurs possibles : <ul style="list-style-type: none"> <li>False : aucune clé ou code d'activation n'a été défini dans l'application.</li> <li>True : une clé ou un code d'activation a été ajouté à l'application.</li> </ul>
LicenseDaysLeft	Affiche le nombre de jours restants avant l'expiration de la licence en cours.	Nombre de jour restants avant l'expiration de la licence en cours; Valeurs non positives possibles : <ul style="list-style-type: none"> <li>0 : licence expirée.</li> <li>-1 : impossible d'obtenir des informations sur la clé active ou la clé indiquée ne peut être utilisée pour activer l'application (par exemple, elle est bloquée sur la base d'une liste noire de clés).</li> </ul>
AVBasesDatetime	L'horodatage de la version actuelle des bases antivirus.	Date et heure de création des bases antivirus actuelles.  Si l'application installée n'utilise pas de bases antivirus, le champ affiche la valeur Pas installé.

Propriété de l'instance	Description	Valeurs
IsExploitPreventionEnabled	Etat du composant Protection contre les exploits.	Etat du composant Protection contre les exploits. Valeurs possibles : <ul style="list-style-type: none"> <li>• True : le composant Protection contre les exploits est activé et offre une protection.</li> <li>• False : le composant Protection contre les exploits n'offre aucune protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.</li> </ul>
ProtectionTasksRunning	L'ensemble des tâches de protection en cours d'exécution.	Liste des tâches de protection, de contrôle et de surveillance en cours d'exécution. Ce champ doit tenir compte de toutes les tâches non périodiques en cours d'exécution. Si une tâche non périodique est en cours d'exécution, le champ a la valeur "Non".
IsAppControlRunning	L'état de la tâche Contrôle du lancement des applications.	Etat de la tâche Contrôle du lancement des applications. <ul style="list-style-type: none"> <li>• True : la tâche Contrôle du lancement des applications est en cours d'exécution.</li> <li>• False : la tâche Contrôle du lancement des applications n'est pas en cours d'exécution ou le composant Contrôle du lancement des applications n'est pas installé.</li> </ul>
AppControlMode	Le mode de tâche du Contrôle du lancement des applications.	Description de l'état actuel du composant Contrôle du lancement des applications et du mode sélectionné pour la tâche correspondante. Valeurs possibles : <ul style="list-style-type: none"> <li>• Active : le mode <b>Actif</b> est sélectionné dans les paramètres de la tâche.</li> <li>• Statistics Only : le mode <b>Statistiques uniquement</b> est sélectionné dans les paramètres de la tâche.</li> <li>• Not installed : le composant Contrôle du lancement des applications n'est pas installé</li> </ul>
AppControlRulesNumber	Nombre total de règles du contrôle du lancement des applications.	Le nombre de règles actuellement définies dans les paramètres de la tâche Contrôle du lancement des applications.

Propriété de l'instance	Description	Valeurs
AppControlLastBlocking	L'horodatage de la dernière interdiction de lancement d'une application par la tâche Contrôle du lancement des applications dans n'importe quel mode.	Date et heure auxquelles le composant Contrôle du lancement des applications a bloqué pour la dernière fois le lancement d'une application. Ce champ reprend toutes les applications bloquées, quel que soit le mode de tâche.  Si aucune instance d'interdiction de lancement d'une application n'est enregistré à l'heure du traitement de la requête WMI, la valeur "No" est attribuée au champ.
PeriodicTasksRunning	L'ensemble des tâches de périodiques en cours d'exécution.	Liste des tâches d'analyse à la demande, de mise à jour et d'inventaire en cours d'exécution. Ce champ doit contenir toutes les tâches périodiques en cours d'exécution.  Si aucune tâche périodique n'est en cours d'exécution, la valeur "No" est attribuée au champ.
ConnectionState	L'état de la connexion entre le composant WMI Provider et le service Kaspersky Security (KAVFS).	Informations relatives à l'état de la connexion entre le module WMI Provider et le service Kaspersky Security. Valeurs possibles : <ul style="list-style-type: none"> <li>• Success : la connexion a été établie : le client WMI peut recevoir les informations relatives à l'état de l'application.</li> <li>• Failed. Code erreur : &lt;code&gt; : impossible d'établir la connexion en raison de l'erreur portant le code indiqué.</li> </ul>

Ces données représentent les propriétés de l'instance KasperskySecurity\_ProductInfo.ProductName=Kaspersky Security où :

- KasperskySecurity\_ProductInfo est le nom de la classe Kaspersky Security for Windows Server class
- .ProductName=Kaspersky Security est le paramètre clé Kaspersky Security for Windows Server

L'instance est créée dans l'espace de noms ROOT\Kaspersky\Security.

# Utilisation de Kaspersky Security for Windows Server depuis la ligne de commande

Cette section décrit l'utilisation de Kaspersky Security for Windows Server via la ligne de commande.

## Contenu du chapitre

Commandes de la ligne de commande .....	<a href="#">569</a>
Codes de retour de la ligne de commande.....	<a href="#">598</a>

## Commandes de la ligne de commande

Vous pouvez exécuter les instructions d'administration de base Kaspersky Security for Windows Server via la ligne de commande du serveur protégé si vous avez inclus le composant Utilitaire de ligne de commande dans la liste des composants à installer lors de l'installation de Kaspersky Security for Windows Server.

La ligne de commande permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Security for Windows Server.

Certaines commandes de Kaspersky Security for Windows Server sont exécutées les modes suivants :

- Mode synchrone : l'administration revient à la console uniquement après la fin de l'exécution de la commande.
- Mode asynchrone : l'administration revient à la console directement après le lancement de la commande.

► *Pour interrompre l'exécution d'une commande en mode synchrone,*

appuyez sur la combinaison de touches **Ctrl+C**.

Respectez les règles suivantes lors de la saisie des instructions de Kaspersky Security for Windows Server :

- Saisissez les paramètres et les instructions 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, saisissez ce nom (et son chemin d'accès) entre guillemets, par exemple : "C:\TEST\test cpp.exe" ;
- le cas échéant, vous pouvez utiliser des caractères génériques dans les noms des fichiers ou des chemins, par exemple : "C:\Temp\Temp\*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp\*.doc"

La ligne de commande vous permet d'effectuer toutes les opérations de gestion et d'administration de Kaspersky Security for Windows Server (cf. tableau ci-dessous).



Tableau 87. Commandes de Kaspersky Security for Windows Server

Instruction	Description
KAVSHELL APPCONTROL (cf. section "Enrichissement de la liste des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL" à la page <a href="#">584</a> )	Enrichit la liste des règles du Contrôle du lancement des applications créées conformément au principe d'ajout sélectionné.
KAVSHELL APPCONTROL /CONFIG (cf. section "Administration de la tâche Contrôle du lancement des applications KAVSHELL APPCONTROL /CONFIG" à la page <a href="#">581</a> )	Gère les modes de fonctionnement de la tâche Contrôle du lancement des applications.
KAVSHELL APPCONTROL /GENERATE (cf. section "Génération des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL /GENERATE" à la page <a href="#">582</a> )	Lance la tâche Génération des règles du Contrôle du lancement des applications.
KAVSHELL VACUUM (cf. section "Défragmentation des fichiers journaux de Kaspersky Security for Windows Server. KAVSHELL VACUUM" à la page <a href="#">594</a> )	Défragmente les fichiers journaux de Kaspersky Security for Windows Server.
KAVSHELL PASSWORD	Administre les paramètres de la protection par mot de passe.
KAVSHELL HELP (cf. section "Affichage de l'aide sur les commandes de Kaspersky Security for Windows Server. KAVSHELL HELP" à la page <a href="#">572</a> )	Affiche l'aide sur les commandes de Kaspersky Security for Windows Server.
KAVSHELL START (cf. section "Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP" on page <a href="#">572</a> )	Lance le Service Kaspersky Security for Windows Server.
KAVSHELL STOP (cf. section "Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP" on page <a href="#">572</a> )	Arrête le Service Kaspersky Security for Windows Server

Instruction	Description
KAVSHELL SCAN (cf. section "Analyse de la zone sélectionnée. KAVSHELL SCAN" à la page <a href="#">573</a> )	Crée et lance une tâche d'analyse à la demande temporaire dont la zone d'analyse et les paramètres de sécurité sont définis par les arguments de l'instruction.
KAVSHELL SCANCritical (cf. section "Lancement de la tâche Analyse des zones critiques. KAVSHELL SCANCritical" à la page <a href="#">577</a> )	Lance la tâche système Analyse des zones critiques.
KAVSHELL TASK (cf. section "Administration de la tâche indiquée en mode asynchrone. KAVSHELL TASK" à la page <a href="#">578</a> )	Lance, suspend/relance, arrête la tâche indiquée en mode asynchrone/rend l'état actuelle de la tâche/les statistiques de la tâche.
KAVSHELL RTP (cf. section "Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP" à la page <a href="#">580</a> )	Lance ou arrête toutes les tâches de protection en temps réel.
KAVSHELL UPDATE (cf. section "Lancement de la tâche de mise à jour des bases de l'application de Kaspersky Security for Windows Server. KAVSHELL UPDATE" à la page <a href="#">586</a> )	Lance la tâche de mise à jour des bases de Kaspersky Security for Windows Server selon les paramètres définis à l'aide des arguments de l'instruction.
KAVSHELL ROLLBACK (cf. section "Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server. KAVSHELL ROLLBACK" à la page <a href="#">589</a> )	Remet les bases à l'état antérieur à la mise à jour.
KAVSHELL LICENSE (cf. section "Activation de l'application KAVSHELL LICENSE" à la page <a href="#">590</a> )	Ajoute ou supprime des clés et des codes d'activation. Affiche des informations sur les clés et codes d'activation ajoutés.
KAVSHELL TRACE (cf. section "Activation, configuration et désactivation de la constitution d'un journal de traçage. KAVSHELL TRACE" à la page <a href="#">591</a> )	Active ou désactive le journal de trace, gère les paramètres du journal de trace.
KAVSHELL DUMP (cf. section "Activation et désactivation de la création de fichiers dump. KAVSHELL DUMP" à la page <a href="#">595</a> )	Active ou désactive la création de fichiers dump de mémoire des processus de Kaspersky Security for Windows Server en cas d'arrêt suite à une erreur.

Instruction	Description
KAVSHELL IMPORT (cf. section "Importation des paramètres. KAVSHELL IMPORT" à la page <a href="#">596</a> )	Importe les paramètres généraux de Kaspersky Security for Windows Server, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration créé au préalable.
KAVSHELL EXPORT (cf. section "Exportation des paramètres. KAVSHELL EXPORT" à la page <a href="#">597</a> )	Exporte tous les paramètres de Kaspersky Security for Windows Server et des tâches existantes dans un fichier de configuration.
KAVSHELL DEVCONTROL(cf. section "Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier. KAVSHELL DEVCONTROL" à la page <a href="#">585</a> )	Enrichit la liste des règles du Contrôle des périphériques créées conformément au principe d'ajout sélectionné.

## Affichage de l'aide sur les commandes de Kaspersky Security for Windows Server. KAVSHELL HELP

Pour obtenir la liste de toutes les instructions de Kaspersky Security for Windows Server, exécutez une des commandes suivantes :

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une commande, exécutez une des commandes suivantes :

```
KAVSHELL HELP <instruction>
```

```
KAVSHELL <instruction> /?
```

### Exemples d'instruction KAVSHELL HELP

Pour consulter des informations plus détaillées sur l'instruction KAVSHELL SCAN, exécutez l'instruction suivante :

```
KAVSHELL HELP SCAN
```

## Lancement et arrêt du Service Kaspersky Security KAVSHELL START, KAVSHELL STOP

Pour lancer le Service Kaspersky Security, exécutez la commande

```
KAVSHELL START
```

Le lancement du Service Kaspersky Security s'accompagne par défaut du lancement des tâches Protection des fichiers en temps réel et Analyse au démarrage du système d'exploitation ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Pour arrêter le Service Kaspersky Security, exécutez la commande

```
KAVSHELL STOP
```

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument [/pwd:<mot de passe>].

## Analyse de la zone indiquée. KAVSHELL SCAN

Pour lancer la tâche d'analyse de secteurs définis du serveur protégé, utilisez l'instruction `KAVSHELL SCAN`. Les arguments de cette commande définissent les paramètres de la zone d'analyse et paramètres de sécurité du nœud sélectionné.

La tâche d'analyse à la demande lancée à l'aide de l'instruction `KAVSHELL SCAN` est temporaire. Elle apparaît dans la console de l'application uniquement pendant son exécution (la console de l'application ne vous permet pas de consulter les paramètres de la tâche). Le journal des performances de la tâche est créé à ce moment. Il apparaît dans le nœud **Journaux d'exécution de la tâche** de la console de l'application.

Vous pouvez employer une variable système pour désigner le chemin dans la tâche d'analyse de zones distinctes. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL SCAN` avec les privilèges de cet utilisateur.

L'instruction `KAVSHELL SCAN` est exécutée en mode synchrone.

Pour lancer une tâche d'analyse à la demande existante via la ligne de commande, utilisez la commande `KAVSHELL TASK` (cf. section "Administration de la tâche indiquée en mode asynchrone. `KAVSHELL TASK`" à la page [578](#)).

### Syntaxe de la commande KAVSHELL SCAN

```
KAVSHELL SCAN <zones d'analyse>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< nom du fichier
contenant la liste des zones d'analyse >] [/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 secondes>]
[/NOICHECKER] [/NOISWIFT] [/ANALYZERLEVEL] [/NOCHECKMSSIGN] [/W:<nom du fichier
journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction `KAVSHELL SCAN` contient les arguments obligatoires et additionnels dont l'utilisation n'est pas obligatoire (cf. tableau ci-dessous).

### Exemples d'instruction KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
```

```
/E:ABM /EM:"*.xtx;*.ff?;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL
/NOISWIFT:1 /W:report.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tableau 88. Arguments de l'instruction KAVSHELL SCAN

Clé	Description
<b>Zone d'analyse.</b> Argument obligatoire.	
<fichiers>	Zone d'analyse : liste de fichiers, de répertoires, de chemins de réseau et de zones prédéfinies. Indiquez les chemins de réseau au format UNC (Universal Naming Convention). Dans l'exemple suivant, le dossier Folder4 est indiqué sans son chemin d'accès. Il se trouve dans le répertoire d'où l'instruction KAVSHELL est exécutée : KAVSHELL SCAN Folder4 Si le nom de l'objet à analyser contient des espaces, il faudra l'indiquer entre guillemets. Si vous avez choisi un dossier, Kaspersky Security for Windows Server analyse également tous les sous-dossiers du dossier en question. Pour analyser un groupe de fichiers, vous pouvez utiliser les caractères * ou ?
<répertoires>	
<chemin de réseau>	
/MEMORY	Analyse les objets dans la mémoire vive.
/SHARED	Analyse les dossiers partagés sur le serveur.
/STARTUP	Analyse les objets de démarrage
/REMDRIVES	Analyse les disques amovibles.
/FIXDRIVES	Analyse les disques durs.
/MYCOMP	Analyse tous les secteurs du serveur protégé.
/L: <nom du fichier contenant la liste des zones d'analyse>	Nom du fichier contenant la liste des zones d'analyse, y compris le chemin d'accès complet au fichier. Les zones d'analyse dans le fichier sont séparées par un retour à la ligne. Vous pouvez indiquer les couvertures d'analyse prédéfinies comme indiqué dans l'exemple ci-après de fichier contenant la liste des zones d'analyse : C:\ D:\Docs\*.doc E:\My Documents /STARTUP /SHARED
<b>Objets à analyser</b> (Types de fichier). Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security for Windows Server analyse les objets en fonction du format.	
/FA	Analyse tous les objets
/FC	Analyse les objets en fonction du format (par défaut). Kaspersky Security for Windows Server analyse uniquement les objets dont le format figure dans la liste des formats des objets infectables.

Clé	Description
/FE	Analyse les objets en fonction de l'extension. Kaspersky Security for Windows Server analyse uniquement les objets dont l'extension figure dans la liste des extensions des objets infectables.
/NEWONLY	Analyser uniquement les nouveaux fichiers et les fichiers modifiés. Si vous n'utilisez pas cet argument, Kaspersky Security for Windows Server analyse tous les objets.
<b>Actions à exécuter sur les objets infectés et autres.</b> Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security for Windows Server applique l'action <b>Ignorer</b> .	
DISINFECT	Désinfecter, ignorer si la désinfection est impossible Les paramètres DISINFECT et DELETE ont été préservés dans la version actuelle de Kaspersky Security for Windows Server pour garantir la compatibilité avec les versions antérieures. Ces paramètres peuvent être utilisés à la place des commandes clés /AI et /AS. Dans ce cas, Kaspersky Security for Windows Server ne traite pas les objets probablement infectés.
DISINFDEL	Désinfecter, supprimer si la désinfection est impossible
DELETE	Supprimer Les paramètres DISINFECT et DELETE ont été préservés dans la version actuelle de Kaspersky Security for Windows Server pour garantir la compatibilité avec les versions antérieures. Ces paramètres peuvent être utilisés à la place des commandes clés /AI et /AS. Dans ce cas, Kaspersky Security for Windows Server ne traite pas les objets probablement infectés.
REPORT	Envoie un rapport (par défaut)
AUTO	Exécuter l'action recommandée
<b>/AS : Actions à exécuter sur les objets probablement infectés/</b> Si vous ne définissez aucune valeur pour cet argument, Kaspersky Security for Windows Server applique l'action <b>Ignorer</b> .	
QUARANTAINE	Quarantaine
DELETE	Supprimer
REPORT	Envoie un rapport (par défaut)
AUTO	Exécuter l'action recommandée
<b>Exclusions</b>	
/E:ABMSPO	L'argument exclut les objets composés des types suivants : A : archives SFX ; B : bases de données d'emails ; M : message de texte plat ; S : archives (y compris les archives SFX) ; P : objets compactés ; O : objets OLE intégrés.
/EM:<"masques">	Exclut les fichiers en fonction du masque. Vous pouvez définir plusieurs masques, par exemple EM:"*.txt;*.png; C:\Videos\*.avi".

Clé	Description
/ET:<nombre de secondes>	<p>Arrête le traitement de l'objet s'il dure plus longtemps que la durée indiquée en secondes.</p> <p>Par défaut, l'analyse n'est pas limitée dans le temps.</p>
/ES:<taille>	<p>Exclut de l'analyse les objets composés dont la taille, en mégaoctets, dépasse la valeur de l'argument &lt;taille&gt;.</p> <p>Kaspersky Security for Windows Server analyse par défaut toutes les tailles d'objet.</p>
/TZOFF	<p>Annule les exclusions de la zone de confiance.</p>
<b>Paramètres avancés (Options)</b>	
/NOICHECKER	<p>Désactive l'utilisation de la technologie iChecker (activée par défaut).</p>
/NOISWIFT	<p>Désactive l'utilisation de la technologie iSwift (activée par défaut).</p>
/ANALYZERLEVEL:<niveau d'analyse>	<p>Activation de l'utilisation de l'analyse heuristique et configuration du niveau d'analyse. Les niveaux d'analyse heuristique suivants sont disponibles :</p> <ul style="list-style-type: none"> <li>1 – superficielle ;</li> <li>2 – moyenne ;</li> <li>3 – minutieuse.</li> </ul> <p>Si vous n'utilisez pas cet argument, Kaspersky Security for Windows Server n'utilise pas l'analyse heuristique.</p>
/ALIAS:<nom alternatif de la tâche>	<p>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 Security for Windows Server.</p> <p>Si cet argument n'est pas défini, la tâche reçoit le nom alternatif scan_&lt;kavshell_pid&gt;, par exemple scan_1234. Dans la Console de l'application, la tâche reçoit le nom Analyser les objets (&lt;date et heure&gt;), par exemple, Analyser les objets 16/8/2007 5:13:14 PM.</p>
Paramètres des journaux d'exécution des tâches (Report settings)	

Clé	Description
/W:<nom du fichier journal d'exécution de la tâche>	<p>Si vous désignez cet argument, Kaspersky Security for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument.</p> <p>Le fichier journal d'exécution de la tâche 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.</p> <p>Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Security for Windows Server dans la console Observateur d'événements.</p> <p>Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours.</p> <p>Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.</p> <p>Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande.</p> <p>Le journal est affiché dans le nœud Journaux d'exécution de la tâche de la console de l'application.</p> <p>Si Kaspersky Security for Windows Server ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche un message d'erreur.</p>
/ANSI	<p>La clé permet d'enregistrer les événements dans le journal d'exécution de la tâche dans l'encodage ANSI.</p> <p>La clé ANSI ne sera pas appliquée, si la clé W n'est pas définie.</p> <p>Si la clé ANSI n'est pas spécifiée, le journal d'exécution de la tâche s'effectue dans l'encodage UNICODE.</p>

## Lancement de la tâche Analyse des zones critiques. KAVSHELL SCANCRITICAL

Utilisez la commande `KAVSHELL SCANCRITICAL` pour lancer la tâche prédéfinie d'analyse à la demande Analyse des zones critiques selon les paramètres définis dans la console de l'application.

### Syntaxe de la commande KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<nom du fichier journal d'exécution de la tâche>]
```

### Exemples d'instruction KAVSHELL SCANCRITICAL

Pour exécuter la tâche d'analyse à la demande Analyse des zones critiques et enregistrer le journal d'exécution de la tâche dans le fichier `scancritical.log` dans le répertoire en cours, exécutez l'instruction suivante :

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Vous pouvez configurer l'emplacement du fichier journal d'exécution de la tâche en fonction de la syntaxe de l'argument (cf. tableau ci-dessous).



Tableau 89. Syntaxe de l'argument /W de la commande `KAVSHELL SCANCritical`

Clé	Description
/W:<nom du fichier journal d'exécution de la tâche>	<p>Si vous désignez cet argument, Kaspersky Security for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument.</p> <p>Le fichier journal d'exécution de la tâche 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.</p> <p>Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de l'application dans la console "Observateur d'événements".</p> <p>Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours.</p> <p>Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.</p> <p>Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande.</p> <p>Le journal est affiché dans le nœud <b>Journaux d'exécution de la tâche</b> de la console de l'application.</p> <p>Si Kaspersky Security for Windows Server ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais affiche un message d'erreur.</p>

## Administration de la tâche indiquée en mode asynchrone. `KAVSHELL TASK`

A l'aide de l'instruction `KAVSHELL TASK`, vous pouvez administrer la tâche indiquée : lancer, suspendre, reprendre ou arrêter la tâche ainsi que consulter son état actuel et ses statistiques. L'instruction est exécutée en mode asynchrone.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

### Syntaxe de la commande `KAVSHELL TASK`

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

### Exemples d'instruction `KAVSHELL TASK`

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

KAVSHELL TASK scan-computer /STATE

L'instruction KAVSHELL TASK peut être exécutée sans clé de licence ou avec une ou plusieurs clés de licence (cf. tableau ci-dessous).

Tableau 90. Arguments de l'instruction KAVSHELL TASK

Clé	Description
Sans argument	Renvoie la liste de toutes les tâches de Kaspersky Security for Windows Server. La liste contient les champs : nom alternatif de la tâche, catégorie de tâche (tâche système et tâche définie par utilisateur) 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 Security for Windows Server. Pour consulter les noms alternatifs des tâches dans Kaspersky Security for Windows Server, saisissez l'instruction 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	Récupère l'état actuel de la tâche (par exemple, <i>Exécution en cours</i> , <i>Complété(e)</i> , <i>En pause</i> , <i>Arrêtée</i> , <i>Echec</i> , <i>Lancement en cours</i> , <i>Restauration en cours</i> ).
/STATISTICS	Affiche les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche jusqu'à ce moment.

Renvoie les codes pour la commande KAVSHELL TASK (cf. section "Codes de retour de l'instruction KAVSHELL TASK" à la page [600](#)).

## Enregistrement de KAVFS en tant que processus protégé par le système. KAVSHELL CONFIG

La commande KAVSHELL CONFIG permet de contrôler l'enregistrement du service Kaspersky Security en tant que processus protégé par le système (Protected Process Light) à l'aide du pilote ELAM, installé dans le système d'exploitation lors de l'installation de l'application.

## Syntaxe de la commande KAVSHELL CONFIG

KAVSHELL CONFIG /PPL:<ON|OFF>

Tableau 91. Arguments de la commande KAVSHELL CONFIG

Clé	Description
/PPL:ON	Enregistre le service Kaspersky Security en tant que PPL.
/PPL:OFF	Supprime l'attribut PPL pour le service Kaspersky Security.

L'application annule automatiquement l'enregistrement du service lorsqu'une des actions suivantes quelconque est réalisée :

- désinstallation de l'application
- mise à niveau de l'application
- installation d'un correctif
- réparation des composants de l'application

Codes de retour de la commande KAVSHELL CONFIG.

## Lancement et arrêt des tâches de protection en temps réel. KAVSHELL RTP

L'instruction KAVSHELL RTP vous permet de lancer ou d'arrêter toutes les tâches de protection en temps réel.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument [/pwd:<mot de passe>].

### Syntaxe de la commande KAVSHELL RTP

KAVSHELL RTP </START | /STOP>

### Exemples d'instruction KAVSHELL RTP

Pour lancer toutes les tâches de protection en temps réel, exécutez l'instruction suivante :

KAVSHELL RTP /START

L'instruction KAVSHELL RTP peut inclure n'importe quel des deux arguments obligatoires (cf. tableau ci-dessous).

Tableau 92. Arguments de l'instruction KAVSHELL RTP

Clé	Description
/START	Lance toutes les tâches de protection en temps réel : Protection des fichiers en temps réel, Monitoring des scripts et Utilisation du KSN.
/STOP	Arrête toutes les tâches de protection en temps réel.

## Administration de la tâche Contrôle du lancement des applications KAVSHELL APPCONTROL /CONFIG

A l'aide de la commande `KAVSHELL APPCONTROL /CONFIG`, vous pouvez configurer le mode de fonctionnement de la tâche Contrôle du lancement des applications et contrôle du chargement des modules DLL.

### Syntaxe de la commande KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config  
/savetofile:<chemin d'accès complet au fichier XML>
```

### Exemples de commande KAVSHELL APPCONTROL /CONFIG

- Pour exécuter la tâche Contrôle du lancement des applications sous le mode **Actif** sans chargement du module DLL et enregistrer les paramètres de la tâche à la fin, exécutez la commande :

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>  
/savetofile:c:\appcontrol\config.xml
```

Vous pouvez configurer les paramètres de la tâche le Contrôle du lancement des applications à l'aide de clés (cf. tableau ci-dessous).

Tableau 93. Arguments de la commande `KAVSHELL APPCONTROL /CONFIG`

Clé	Description
<code>/mode:&lt;applyrules statistics&gt;</code>	Mode de fonctionnement de la tâche Contrôle du lancement des applications. Vous avez le choix entre les modes suivants de fonctionnement de la tâche : <ul style="list-style-type: none"> <li>• actif : appliquer les règles du Contrôle du lancement des applications ;</li> <li>• statistics : statistiques uniquement.</li> </ul>
<code>/dll:&lt;no yes&gt;</code>	Désactiver ou activer le contrôle du chargement des modules DLL.
<code>/savetofile: &lt;chemin d'accès complet au fichier XML&gt;</code>	Exporter les règles précisées dans le fichier indiqué au format XML.
<code>/savetofile: &lt;nom complet du fichier XML&gt;</code>	Enregistrez la liste des règles dans un fichier.
<code>/savetofile: &lt;nom complet du fichier XML&gt; /sdc</code>	Enregistrez la liste des règles du contrôle de la distribution des logiciels.
<code>/clearsdc</code>	Supprimez de la liste toutes les règles du contrôle de la distribution des logiciels.

## Génération des règles du contrôle du lancement des applications KAVSHELL APPCONTROL /GENERATE

La commande `KAVSHELL APPCONTROL /GENERATE` permet de composer la liste des règles du Contrôle du lancement des applications.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

### Syntaxe de la commande KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <chemin d'accès au dossier> | /source:<chemin
d'accès au fichier contenant la liste des dossiers> [/masks:<edms>] [/runapp]
[/rules:<ch|cp|h>] [/strong] [/user:<utilisateur ou groupe d'utilisateurs>]
[/export:<chemin d'accès complet au fichier XML>] [/import:<a|r|m>]
[/prefix:<préfixe pour les noms de règles>] [/unique]
```

### Exemples de commande KAVSHELL APPCONTROL /GENERATE

- Pour créer des règles pour les fichiers des dossiers sélectionnés, exécutez la commande :

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

- Pour créer les règles pour les fichiers exécutables de toutes les extensions accessibles dans le dossier indiqué et enregistrer à la fin de la tâche les règles créées dans le fichier indiqué au format XML, exécutez la commande :

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c:\rules\appctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez configurer les paramètres de création automatique des règles du Contrôle du lancement des applications (cf. tableau ci-après).

Tableau 94. Arguments de la commande `KAVSHELL APPCONTROL /GENERATE`

Clé	Description
<b>Zone d'application des règles d'autorisation</b>	
<chemin d'accès au dossier>	Indiquer le chemin d'accès au dossier qui contient les fichiers exécutables pour lesquels il faut créer automatiquement des règles d'autorisation.
/source: <chemin d'accès à la liste des dossiers>	Indiquer le chemin d'accès au fichier TXT qui contient la liste des dossiers avec les fichiers exécutables pour lesquels il faut créer automatiquement les règles d'autorisation.

/masks: <edms>	<p>Indiquer les extensions des fichiers exécutables pour lesquels il faut créer des règles d'autorisation du Contrôle du lancement des applications.</p> <p>Vous pouvez inclure dans la zone d'application des règles créées les fichiers portant les extensions suivantes :</p> <ul style="list-style-type: none"> <li>• e - fichiers portant l'extension exe ;</li> <li>• d - fichiers portant l'extension dll ;</li> <li>• m - fichiers portant l'extension msi ;</li> <li>• s - scripts.</li> </ul>
/runapp	Tenir compte lors de la création des règles d'autorisation des applications lancées sur le serveur protégé au moment de l'exécution de la tâche.
<b>Actions lors de la génération automatique de règles d'autorisation</b>	
/rules: <ch cp h>	<p>Indiquer les actions que la tâche réalise pendant la création des règles d'autorisation du Contrôle du lancement des applications :</p> <ul style="list-style-type: none"> <li>• ch – utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser le hash SHA256.</li> <li>• cp – utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser la valeur du chemin d'accès au fichier exécutable.</li> <li>• h – utiliser le hash SHA256.</li> </ul>
/strong	Utiliser l'en-tête et l'empreinte du certificat numérique lors de la création automatique des règles d'autorisation du Contrôle du lancement des applications. La commande est exécutée si la clé /rules: <ch cp> est spécifiée.
/user: <utilisateur ou groupe d'utilisateurs>	Indiquer le nom d'utilisateur ou du groupe d'utilisateurs auxquels la règle sera appliquée. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini.
<b>Actions à réaliser à la fin de la Génération des règles du Contrôle du lancement des applications</b>	
/export: <chemin d'accès complet au fichier XML>	Enregistrer les règles créées dans un fichier au format XML.
/unique	Ajouter des informations relatives au serveur dotés des applications qui servent à créer les règles d'autorisation du Contrôle du lancement des applications.
/prefix: <préfixe des noms des règles>	Définir le préfixe pour les noms des règles d'autorisation du Contrôle du lancement des applications.

<pre>/import: &lt;a r m&gt;</pre>	<p>Importe les règles créées dans la liste des règles définies du Contrôle du lancement des applications conformément au principe défini d'ajout de nouvelles règles :</p> <ul style="list-style-type: none"> <li>• <b>a - Ajouter aux règles existantes</b> (les règles identiques apparaissent en double) ;</li> <li>• <b>r - Remplacer les règles existantes</b> (les nouvelles règles remplacent les règles définies) ;</li> <li>• <b>m - Fusionner avec les règles existantes</b> (les nouvelles règles dont les paramètres ne correspondent pas aux paramètres des règles déjà créées sont ajoutées).</li> </ul>
-----------------------------------	--

## Enrichissement de la liste des règles du Contrôle du lancement des applications KAVSHELL APPCONTROL

La commande `KAVSHELL APPCONTROL` permet d'ajouter des règles du fichier XML à la liste des règles de la tâche Contrôle du lancement des applications conformément au principe choisi et de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

### Syntaxe de la commande KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

### Exemples d'instruction KAVSHELL APPCONTROL

- *Pour ajouter des règles depuis un fichier au format XML aux règles définies du contrôle du lancement des applications selon le principe Ajouter aux règles existantes, procédez comme suit :*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez sélectionner le principe d'ajout de nouvelles règles au départ d'un fichier désigné au format XML à la liste des règles définies de la tâche Contrôle du lancement des applications (cf. ill. ci-dessous).

Tableau 95. Arguments de la commande `KAVSHELL APPCONTROL`

Clé	Description
<pre>/append &lt;chemin d'accès complet au fichier XML&gt;</pre>	<p>Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Ajouter aux règles existantes</b> (les règles identiques apparaissent en double).</p>

/replace <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Remplacer les règles existantes</b> (les nouvelles règles remplacent les règles définies).
/merge <chemin d'accès complet au fichier XML>	Ajouter à la liste des règles du Contrôle du lancement des applications les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Fusionner avec les règles existantes</b> (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
/clear	Purger la liste des règles du Contrôle du lancement des applications.

## Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier. KAVSHELL DEVCONTROL

La commande `KAVSHELL DEVCONTROL` permet d'ajouter des règles à la liste des règles de la tâche Contrôle des périphériques au départ d'un fichier du format XML conformément au principe choisi ainsi que de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument `[/pwd:<mot de passe>]`.

### Syntaxe de la commande KAVSHELL APPCONTROL

```
KAVSHELL DEVCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

### Exemples d'instruction KAVSHELL DEVCONTROL

- *Pour ajouter des règles depuis un fichier au format XML aux règles définies du contrôle des périphériques selon le principe **Ajouter aux règles existantes**, procédez comme suit :*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

En fonction de la syntaxe des arguments, vous pouvez sélectionner le principe d'ajout de nouvelles règles à la liste des règles définies de la tâche Contrôle des périphériques au départ d'un fichier désigné au format XML (cf. ill. ci-dessous).



Tableau 96. Arguments de la commande `KAVSHELL DEVCONTROL`

Clé	Description
<code>/append &lt;chemin d'accès complet au fichier XML&gt;</code>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Ajouter aux règles existantes</b> (les règles identiques apparaissent en double).
<code>/replace &lt;chemin d'accès complet au fichier XML&gt;</code>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Remplacer les règles existantes</b> (les nouvelles règles remplacent les règles définies).
<code>/merge &lt;chemin d'accès complet au fichier XML&gt;</code>	Ajouter à la liste des règles du Contrôle des périphériques les règles tirées du fichier XML indiqué. Principe d'ajout - <b>Fusionner avec les règles existantes</b> (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
<code>/clear</code>	Purger la liste des règles du Contrôle des périphériques.

## Lancement de la tâche de mise à jour des bases de l'application de Kaspersky Security for Windows Server. `KAVSHELL UPDATE`

La commande `KAVSHELL UPDATE` vous permet de lancer la tâche de mise à jour des bases de Kaspersky Security for Windows Server en mode synchrone.

La tâche de mise à jour des bases de données de Kaspersky Security for Windows Server, lancée à l'aide de la commande `KAVSHELL UPDATE`, est une tâche temporaire. Elle est affichée dans la console de l'application uniquement pendant son exécution. Le journal d'exécution de la tâche est créé à ce moment. Il apparaît dans le nœud **Journaux d'exécution de la tâche** de la console de l'application. Les stratégies de Kaspersky Security Center peuvent s'appliquer aux tâches de mise à jour créées et lancées via la commande `KAVSHELL UPDATE`, ainsi qu'aux tâches de mises à jour créées dans la console de l'application. Pour en savoir plus sur l'administration de Kaspersky Security for Windows Server sur les ordinateurs à l'aide de Kaspersky Security Center, lisez la section "Administration de Kaspersky Security for Windows Server via Kaspersky Security Center".

Vous pouvez utiliser des variables système pour indiquer la source des mises à jour dans cette tâche. Si vous utilisez une variable système définie par l'utilisateur, exécutez l'instruction `KAVSHELL UPDATE` avec les privilèges de cet utilisateur.

### 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:<code iso3166>]
[/W:<nom du fichier journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction KAVSHELL UPDATE contient les arguments obligatoires et les arguments complémentaires dont l'utilisation facultative (cf. tableau ci-dessous).

## Exemples d'instruction KAVSHELL UPDATE

- Pour lancer une tâche de mise à jour des bases de l'application définie par l'utilisateur, exécutez l'instruction suivante :

```
KAVSHELL UPDATE
```

- Pour lancer une tâche de mise à jour des bases de l'application dont les fichiers de mise à jour se trouvent dans le dossier \\server\bases, exécutez l'instruction suivante :

```
KAVSHELL UPDATE \\server\bases
```

- Pour lancer une tâche de mise à jour depuis le serveur FTP <ftp://dnl-ru1.kaspersky-labs.com/> et enregistrer tous les événements de la tâche dans le fichier journal c:\update\_report.log, exécutez l'instruction suivante :

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- Pour recevoir les mises à jour des bases de l'application Kaspersky Security for Windows Server depuis le serveur de mise à jour de Kaspersky Lab ; connectez-vous à la source des mises à jour via le serveur proxy (adresse du serveur proxy : proxy.company.com, port : 8080) ; pour accéder au serveur, utilisez l'authentification intégrée de Microsoft Windows (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser, mot de passe : 123456), puis exécutez l'instruction suivante :

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1  
/PROXYUSER:inetuser /PROXYPWD:123456 :
```

Tableau 97. Arguments de la commande KAVSHELL UPDATE

Clé	Description
<b>Source des mises à jour</b> (clé obligatoire). Indiquez une ou plusieurs sources. Kaspersky Security for Windows Server 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 dossier de mise à jour réseau au format UNC.
<URL>	Source de mises à jour définies par l'utilisateur. adresse du serveur FTP ou HTTP sur lequel se trouve le dossier contenant les mises à jour.
<Dossier local>	Source de mises à jour définies par l'utilisateur. Dossier sur le serveur protégé.
/AK	Serveur d'administration de Kaspersky Security Center en guise de source des mises à jour
/KL	Serveurs de mise à jour de Kaspersky Lab en guise de source des mises à jour
/NOUSEKL	N'utilise pas les serveurs de mise à jour de Kaspersky Lab si les autres sources des mises à jour indiquées sont inaccessibles (utilisés par défaut).
<b>Paramètres du serveur proxy</b>	

Clé	Description
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas cette clé, Kaspersky Security for Windows Server identifiera automatiquement les paramètres du serveur proxy utilisé dans le réseau local.
/AUTHTYPE:<0-2>	Cet argument définit la méthode d'authentification pour l'accès au serveur proxy. Le paramètre peut prendre les valeurs suivantes : <b>0</b> : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Security for Windows Server contactera le serveur proxy sous le compte <b>Système local (SYSTÈME)</b> ; <b>1</b> : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Security for Windows Server contactera le serveur proxy sous le compte dont le nom d'utilisateur et le mot de passe sont définis par les clés /PROXYUSER et /PROXYPWD. <b>2</b> : authentification selon le nom et le mot de passe de l'utilisateur définis par les clés /PROXYUSER et /PROXYPWD (Basic authentication). Si l'accès au serveur proxy ne requiert pas l'authentification, il n'est pas nécessaire d'indiquer cet argument.
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, les arguments /PROXYUSER:<nom d'utilisateur> et /PROXYPWD:<mot de passe> sont ignorés.
/PROXYPWD:<mot de passe>	Mot de passe de l'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez l'argument /AUTHTYPE:0, les arguments /PROXYUSER:<nom d'utilisateur> et /PROXYPWD:<mot de passe> sont ignorés. Si vous définissez l'argument /PROXYUSER mais pas l'argument /PROXYPWD, 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 <b>Ne pas utiliser le serveur proxy pour les adresses locales</b> est appliquée.
<b>Paramètres généraux du serveur FTP ou HTTP</b>	
/NOFTPPASSIVE	Si vous utilisez cet argument, Kaspersky Security for Windows Server utilisera le mode actif du serveur FTP pour se connecter au serveur protégé. Si vous ne définissez pas cet argument, Kaspersky Security for Windows Server utilisera le mode de serveur FTP passif si cela est possible.
/TIMEOUT:<nombre de secondes>	Délai d'attente lors de la connexion au serveur FTP ou HTTP. Si vous n'utilisez pas cette clé, Kaspersky Security for Windows Server utilisera la valeur par défaut : 10 s. Vous ne pouvez entrer que des nombres entiers.

Clé	Description
/REG:<code iso3166>	<p>Paramètres régionaux. Cet argument intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab. Kaspersky Security for Windows Server optimise le téléchargement des mises à jour sur le serveur protégé en choisissant le serveur de mise à jour le plus proche.</p> <p>En guise de 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 ignorez cette clé ou si vous indiquez un code de pays incorrect, Kaspersky Security for Windows Server identifiera l'emplacement du serveur protégé à l'aide des paramètres régionaux de l'ordinateur doté de la console de l'application.</p>
/ALIAS:<nom alternatif de la tâche>	<p>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 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 Security for Windows Server.</p> <p>Si cet argument n'est pas défini, la tâche reçoit le nom alternatif update_&lt;kavshell_pid&gt;, par exemple update_1234. Dans la Console de l'application, la tâche reçoit automatiquement le nom Update-databases (&lt;date heure&gt;), par exemple, Update-databases 16/8/2007 05:41:02 PM.</p>
/W:<nom du fichier journal d'exécution de la tâche>	<p>Si vous désignez cet argument, Kaspersky Security for Windows Server enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par l'argument.</p> <p>Le fichier journal d'exécution de la tâche 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.</p> <p>Le journal reprend les événements définis par les paramètres des journaux d'exécution des tâches et le journal des événements de Kaspersky Security for Windows Server dans la console "Observateur d'événements".</p> <p>Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours.</p> <p>Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.</p> <p>Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande.</p> <p>Le journal est affiché dans le nœud <b>Journaux d'exécution de la tâche</b> de la console de l'application.</p> <p>Si Kaspersky Security for Windows Server ne parvient pas à créer le fichier journal, il n'interrompt pas l'exécution de l'instruction mais n'affiche pas de message sur l'erreur.</p>

Codes de retour de l'instruction KAVSHELL UPDATE (à la page [601](#)).

## Annulation des mises à jour des bases de l'application Kaspersky Security for Windows Server. KAVSHELL ROLLBACK

L'instruction `KAVSHELL ROLLBACK` vous permet d'exécuter la tâche système d'annulation de la mise à jour des bases de données de Kaspersky Security for Windows Server (rétablissement de Kaspersky Security for Windows Server à la version installée antérieurement). La commande est exécutée en mode synchrone.

### Syntaxe de la commande

KAVSHELL ROLLBACK

Codes de retour de l'instruction KAVSHELL ROLLBACK (cf. page [602](#))

## Gestion de l'inspection des journaux. KAVSHELL TASK LOG-INSPECTOR

La commande `KAVSHELL TASK LOG-INSPECTOR` permet de surveiller l'intégrité de l'environnement sur la base de l'analyse du journal des événements Windows.

### Syntaxe de la commande

KAVSHELL TASK LOG-INSPECTOR

### Exemples de commandes

KAVSHELL TASK LOG-INSPECTOR /stop

Tableau 98. Syntaxe de la commande KAVSHELL TASK LOG-INSPECTOR

Clé	Description
/START	Lance la tâche indiquée en mode asynchrone
/STOP	Arrête la tâche indiquée
/STATE	Récupère l'état actuel de la tâche (par exemple, <i>Exécution en cours</i> , <i>Complété(e)</i> , <i>En pause</i> , <i>Arrêtée</i> , <i>Echec</i> , <i>Lancement en cours</i> , <i>Restauration en cours</i> ).
/STATISTICS	Affiche les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche jusqu'à ce moment.

Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR (cf. section "Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR" à la page [600](#)).

## Activation de l'application KAVSHELL LICENSE

La commande `KAVSHELL LICENSE` permet de gérer les clés et les codes d'activation de Kaspersky Security for Windows Server.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument [/pwd:<mot de passe>].

### Syntaxe de la commande KAVSHELL LICENSE

KAVSHELL LICENSE [/ADD:<fichier clé | code d'activation> [/R] | /DEL:<clé | numéro du code d'activation>]

## Exemples d'instruction KAVSHELL LICENSE

► Pour activer l'application, exécutez la commande :

```
KAVSHELL.EXE LICENSE / ADD: <code d'activation ou clé>
```

► Pour obtenir les informations sur les clés ajoutées, exécutez l'instruction suivante :

```
KAVSHELL LICENSE
```

► Pour supprimer la clé ajoutée avec le numéro de série 0000-000000-00000001, exécutez l'instruction suivante :

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

L'instruction `KAVSHELL LICENSE` peut être exécutée avec ou sans les clés de licence (cf. tableau ci-dessous).

Tableau 99. Arguments de la commande `KAVSHELL LICENSE`

Clé	Description
Sans argument	L'instruction affiche les informations suivantes sur les clés ajoutées : <ul style="list-style-type: none"> <li>• Clé.</li> <li>• Type de licence (commerciale).</li> <li>• Durée de validité de la licence associée à la clé.</li> <li>• Etat de la clé (active ou complémentaire). Si la valeur * est définie, la clé ajoutée est une clé additionnelle.</li> </ul>
/ADD:<nom du fichier clé ou code d'activation>	Ajoute la clé à l'aide du fichier ou du code d'activation indiqué. Pour désigner le chemin d'accès au fichier clé, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
/R	Le code d'activation ou la clé /R vient compléter le code d'activation ou la clé /ADD et signale que ce code d'activation ou cette clé est ajout en tant que clé ou code complémentaire.
/DEL:<clé ou du code d'activation>	Supprime la clé portant le numéro indiqué ou le code d'activation indiqué.

Renvoie les codes pour la commande `KAVSHELL LICENSE` (cf. section "Codes de retour de l'instruction `KAVSHELL LICENSE`" à la page [602](#)).

## Activation, configuration et désactivation d'un journal de traçage. KAVSHELL TRACE

L'instruction `KAVSHELL TRACE` vous permet d'activer ou de désactiver la création d'un journal de traçage pour tous les sous-systèmes de Kaspersky Security for Windows Server ainsi que de définir le niveau de détail des informations reprises dans le journal.

Kaspersky Security for Windows Server consigne les informations dans les fichiers de trace et le fichier dump en clair.

### Syntaxe de la commande KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<dossier contenant les fichiers journaux de traçage>  
[/S:<taille maximale du fichier de trace en mégaoctets>]  
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Si le journal de traçage est constitué et vous souhaitez modifier ses paramètres, saisissez l'instruction `KAVSHELL TRACE` avec l'argument `/ON` et définissez les paramètres du journal de traçage à l'aide des arguments `/S` et `/LVL` (cf. tableau ci-dessous).

Tableau 100. Arguments de la commande KAVSHELL TRACE

Clé	Description
/ON	Active la constitution du journal de traçage.
/F:<dossier contenant les fichiers journaux de traçage>	<p>Cet argument indique le chemin d'accès complet au dossier dans lequel les fichiers journaux de traçage seront conservés (argument obligatoire).</p> <p>Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Les chemins d'accès aux dossiers sur les lecteurs réseau d'autres serveurs non protégés ne peuvent pas être précisés.</p> <p>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".</p> <p>Pour désigner le chemin d'accès au dossier contenant les fichiers journaux de traçage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur</p>
/S:<Taille maximale du fichier journal en mégaoctets>	<p>Cet argument définit la taille maximale d'un fichier journal de traçage. Dès que la taille du fichier journal atteint la valeur maximale, Kaspersky Security for Windows Server consigne les informations dans un nouveau fichier ; le fichier journal antérieur est enregistré.</p> <p>Si vous ne définissez pas cet argument, la taille maximale d'un fichier journal sera limitée à 50 Mo.</p>
/LVL:debug info warning error critical	<p>Cette clé définit le niveau de détail du journal depuis le niveau le plus détaillé (<b>Toutes les informations de débogage</b>) où tous les événements sont enregistrés dans le journal jusqu'au niveau minimum (<b>Événements critiques</b>) où seuls les événements critiques sont enregistrés.</p> <p>Si vous ne définissez pas cette clé, le journal de trace contiendra les événements correspondant au niveau de détail <b>Toutes les informations de débogage</b>.</p>
/OFF	Cet argument désactive la constitution du journal de traçage.

### Exemples d'instruction KAVSHELL TRACE

- Pour activer le journal de trace avec le niveau de détail **Toutes les informations de débogage** et la taille maximale du fichier journal de 200 Mo et enregistrer le fichier journal dans le répertoire C:\Trace Folder, exécutez la commande suivante :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

- Pour activer le journal de trace avec le niveau de détail **Événements importants** et enregistrer le fichier journal dans le dossier C:\Trace Folder, exécutez la commande :

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```



- Pour désactiver le contenu du journal de traçage, exécutez l'instruction suivante :

```
KAVSHELL TRACE OFF
```

Renvoie les codes pour la commande KAVSHELL TRACE (cf. section "Codes de retour de l'instruction KAVSHELL TRACE" à la page [603](#)).

## Défragmentation des fichiers journaux de Kaspersky Security for Windows Server. KAVSHELL VACUUM

La commande KAVSHELL VACUUM permet de défragmenter les fichiers journaux des événements de l'application. Il permet d'éviter les erreurs système et d'application provoquées par le stockage d'un grand nombre de fichiers journaux créés suite aux événements de l'application.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument [/pwd:<mot de passe>].

Il est conseillé d'appliquer la commande KAVSHELL VACUUM pour optimiser la taille des fichiers journaux en cas d'exécution fréquente des tâches d'analyse à la demande et des tâches de mise à jour. Lors de l'exécution de la commande, Kaspersky Security for Windows Server met à jour la structure logique des fichiers journaux de l'application enregistrés sur un serveur protégé au chemin d'accès indiqué.

Par défaut, les fichiers journaux de l'application sont conservés à l'emplacement C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports. Si vous avez désigné un autre chemin d'accès manuellement pour le stockage des journaux, la commande KAVSHELL VACUUM exécute une défragmentation des fichiers dans le dossier que vous aurez désigné dans les paramètres des journaux de Kaspersky Security for Windows Server.

Des fichiers journaux des événements de grande taille à défragmenter augmente la durée d'exécution de la commande KAVSHELL VACUUM.

Pendant l'exécution de la commande KAVSHELL VACUUM, l'exécution des tâches de protection en temps réel et de contrôle du serveur est impossible. La procédure de défragmentation bloque l'accès au journal e Kaspersky Security for Windows Server et interdit l'enregistrement des événements dans le journal. Afin d'éviter de réduire le niveau de sécurité de l'ordinateur, il est conseillé de planifier l'exécution de la commande KAVSHELL VACUUM en dehors des heures de bureau.

- Pour défragmenter les fichiers journaux créés suite aux événements survenus pendant l'utilisation de Kaspersky Security for Windows Server, exécutez la commande :

```
KAVSHELL VACUUM
```

L'exécution de la commande est accessible en cas de lancement sous les autorisations du compte utilisateur de l'administrateur local.

## Purge de la base iSwift. KAVSHELL FBRESET

Kaspersky Security for Windows Server utilise la technologie iSwift qui permet de ne pas devoir analyser à nouveau un fichier si celui-ci n'a pas été modifié depuis l'analyse antérieure (**Utiliser la technologie iSwift**).

Kaspersky Security for Windows Server crée dans le dossier système %SYSTEMDRIVE%\System Volume Information les fichiers klamfb.dat et klamfb2.dat qui contiennent des informations relatives aux objets sains déjà analysés. Plus le nombre de fichiers différents analysés par Kaspersky Security for Windows Server est élevé, plus la taille du fichier klamfb.dat (klamfb2.dat) augmente. Ce fichier contient uniquement les informations actuelles sur les fichiers existant dans le système : si un fichier quelconque est supprimé, Kaspersky Security for Windows Server supprime les informations qui le concerne dans le fichier klamfb.dat.

Pour purger ce fichier, utilisez l'instruction `KAVSHELL FBRESET`.

Tenez compte des particularités suivantes de l'instruction `KAVSHELL FBRESET` :

- Lors de la purge du fichier klamfb.dat à l'aide de l'instruction `KAVSHELL FBRESET`, Kaspersky Security for Windows Server ne suspend pas la protection (à la différence de la suppression manuelle du fichier).
- Après la purge du fichier klamfb.dat, Kaspersky Security for Windows Server peut augmenter la charge sur le serveur. Dans ce cas, Kaspersky Security for Windows Server analyse tous les fichiers sollicités pour la première fois après la purge du fichier klamfb.dat. Après l'analyse, Kaspersky Security for Windows Server introduit à nouveau dans le fichier klamfb.dat les informations relatives à chaque objet analysé. Lorsque cet objet sera à nouveau sollicité, la technologie iSwift permet de ne pas devoir l'analyser à nouveau, pour autant qu'il n'ait pas été modifié.

L'exécution de la commande `KAVSHELL FBRESET` requiert le lancement de la ligne de code sous le compte utilisateur SYSTEM.

## Activation et désactivation de la création de fichiers dump. KAVSHELL DUMP

L'instruction `KAVSHELL DUMP` permet d'activer ou de désactiver la création de modèles de mémoire (fichier dump) des processus de Kaspersky Security for Windows Server en cas d'arrêt provoqué par une erreur (cf. tableau ci-dessous). De plus, vous pouvez prendre à n'importe quel moment un instantané de la mémoire des processus de Kaspersky Security for Windows Server en cours d'exécution.

Pour obtenir le fichier dump, la commande `KAVSHELL DUMP` doit être lancée sous le compte système local (SYSTEM).

## Syntaxe de la commande KAVSHELL DUMP

KAVSHELL DUMP </ON /F:<dossier contenant le fichier dump>|/SNAPSHOT /F:<dossier contenant le fichier dump> / P:<pid> | /OFF>

Tableau 101. Arguments de la commande KAVSHELL DUMP

Clé	Description
/ON	Active la création d'un fichier dump du processus en cas d'arrêt suite à une erreur.
/F:<dossier contenant les fichiers dump>	Cet argument est obligatoire. Il indique le chemin d'accès au répertoire où le fichier dump sera enregistré. Les chemins d'accès aux dossiers sur les lecteurs réseau d'autres serveurs non protégés ne peuvent pas être précisés. Pour désigner le chemin d'accès au dossier contenant le fichier dump, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
/SNAPSHOT	Crée un instantané du modèle de mémoire du processus en exécution indiqué et enregistre le fichier dump 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 fichier dump en cas d'arrêt suite à une erreur.

Renvoie les codes pour la commande KAVSHELL DUMP (cf. section "Codes de retour de l'instruction KAVSHELL DUMP" à la page [603](#)).

## Exemples d'instruction KAVSHELL DUMP

- Pour activer la création d'un fichier dump ; enregistrer le fichier dump dans le répertoire C:\Dump, exécutez la commande suivante :

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

- Pour enregistrer une image de la mémoire du processus avec l'identifiant 1234 dans le répertoire C:/Dumps, exécutez l'instruction suivante :

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

- Pour désactiver la création d'un fichier dump, exécutez la commande suivante :

```
KAVSHELL DUMP OFF
```

## Importation des paramètres. KAVSHELL IMPORT

L'instruction KAVSHELL IMPORT permet d'importer les paramètres de Kaspersky Security for Windows Server, de ses fonctions et de ses tâches depuis un fichier de configuration dans Kaspersky Security for Windows Server sur le serveur protégé. Vous pouvez créer le fichier de configuration à l'aide de l'instruction KAVSHELL EXPORT.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez l'argument [/pwd:<mot de passe>].

### Syntaxe de la commande KAVSHELL IMPORT

KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>

### Exemples d'instruction KAVSHELL IMPORT

KAVSHELL IMPORT Host1.xml

Tableau 102. Arguments de la commande KAVSHELL IMPORT

Clé	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration d'où les paramètres vont être importés. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Renvoie les codes pour la commande KAVSHELL IMPORT (cf. section "Codes de retour de l'instruction KAVSHELL IMPORT" à la page [604](#)).

## Exportation des paramètres. KAVSHELL EXPORT

L'instruction KAVSHELL EXPORT permet d'exporter tous les paramètres de Kaspersky Security for Windows Server et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Security for Windows Server sur d'autres serveurs.

### Syntaxe de la commande KAVSHELL EXPORT

KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>

### Exemples d'instruction KAVSHELL EXPORT

KAVSHELL EXPORT Host1.xml

Tableau 103. Arguments de la commande KAVSHELL EXPORT

Clé	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. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Renvoie les codes pour la commande KAVSHELL EXPORT (cf. section "Codes de retour de l'instruction KAVSHELL EXPORT" à la page [604](#)).

## Intégration avec Microsoft Operation Management Suite. KAVSHELL OMSINFO

A l'aide de la commande KAVSHELL OMSINFO, vous pouvez réviser l'état de l'application et les informations sur

les menaces détectées par les bases antivirus et le service KSN. Les données sur les menaces proviennent des journaux des événements disponibles.

### Syntaxe de la commande KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <chemin et nom du fichier généré>
```

### Exemples d'instruction KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tableau 104. Arguments de la commande KAVSHELL OMSINFO

Clé	Description
<chemin et nom du fichier généré>	Nom du fichier généré qui contient des informations sur l'état de l'application et les menaces détectées.

## Codes de retour de la ligne de commande

### Dans cette section

Codes de retour des instructions KAVSHELL START et KAVSHELL STOP .....	<a href="#">599</a>
Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCritical .....	<a href="#">599</a>
Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR .....	<a href="#">600</a>
Codes de retour de l'instruction KAVSHELL TASK .....	<a href="#">600</a>
Codes de retour de l'instruction KAVSHELL RTP .....	<a href="#">601</a>
Codes de retour de l'instruction KAVSHELL UPDATE .....	<a href="#">601</a>
Codes de retour de l'instruction KAVSHELL ROLLBACK .....	<a href="#">602</a>
Codes de retour de l'instruction KAVSHELL LICENSE .....	<a href="#">602</a>
Codes de retour de l'instruction KAVSHELL TRACE .....	<a href="#">603</a>
Codes de retour de l'instruction KAVSHELL FBRESET .....	<a href="#">603</a>
Codes de retour de l'instruction KAVSHELL DUMP .....	<a href="#">603</a>
Codes de retour de l'instruction KAVSHELL IMPORT .....	<a href="#">604</a>
Codes de retour de l'instruction KAVSHELL EXPORT .....	<a href="#">604</a>

## Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Tableau 105. Codes de retour des instructions KAVSHELL START et KAVSHELL STOP

Code de retour	Description
0	L'opération a réussi
-3	Erreur de privilèges d'accès
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (par exemple, le service de Kaspersky Security for Windows Server est déjà exécuté ou est déjà arrêté)
-7	Le service n'est pas enregistré
-8	Le lancement automatique du service est désactivé
-9	La tentative de démarrage de l'ordinateur sous un autre compte utilisateur a échoué (par défaut, le service de Kaspersky Security for Windows Server fonctionne sous le compte utilisateur Système local).
-99	Erreur inconnue

## Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCritical

Tableau 106. Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCritical

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 zones d'analyse est introuvable).
-5	Syntaxe de la commande incorrecte ou zone d'analyse non définie.
-80	Objets infectés et autres détectés
-81	Objets probablement infectés détectés
-82	Des erreurs de traitement ont été découvertes
-83	Des objets non analysés ont été découverts
-84	Objets endommagés détectés

Code de retour	Description
-85	Impossible de créer le fichier journal d'exécution de la tâche
-99	Erreur inconnue
-301	Clé non valide

## Codes de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR

Tableau 107. Code de retour de l'instruction KAVSHELL TASK LOG-INSPECTOR

Code de retour	Description
0	L'opération a réussi
-6	Opération invalide (par exemple, le service de Kaspersky Security for Windows Server est déjà exécuté ou est déjà arrêté)
402	La tâche est déjà lancée (pour l'argument /STATE)

## Codes de retour de l'instruction KAVSHELL TASK

Tableau 108. Codes de retour de l'instruction 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 non valide
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 l'instruction KAVSHELL RTP

Tableau 109. Codes de retour de l'instruction 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 non valide

## Codes de retour de l'instruction KAVSHELL UPDATE

Tableau 110. Codes de retour de l'instruction 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 d'extension ne sont pas présents dans la source indiquée ou leur format est inconnu
-209	Erreur de connexion à la source des mises à jour
-232	Erreur d'authentification lors de la connexion au serveur proxy
-234	Erreur de connexion à l'application Kaspersky Security Center
-235	Kaspersky Security for Windows Server n'a pas subi d'authentification lors de la connexion à la source des mises à jour



Code de retour	Description
-236	Les bases de Kaspersky Embedded Systems Security sont endommagées
-301	Clé non valide

## Codes de retour de l'instruction KAVSHELL ROLLBACK

Tableau 111. Codes de retour de l'instruction 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 l'instruction KAVSHELL LICENSE

Tableau 112. Codes de retour de l'instruction 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
-4	Clé portant le numéro indiqué introuvable
-5	Syntaxe de la commande incorrecte
-6	Opération incorrecte (la clé a déjà été ajoutée)
-99	Erreur inconnue
-301	Clé non valide
-303	Licence destinée à une autre application

## Codes de retour de l'instruction KAVSHELL TRACE

Tableau 113. Codes de retour de l'instruction 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 journaux de traçage est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (tentative d'exécution de la commande KAVSHELL TRACE /OFF si la création du journal de traçage a déjà été désactivée)
-99	Erreur inconnue

## Codes de retour de l'instruction KAVSHELL FBRESET

Tableau 114. Codes de retour de l'instruction KAVSHELL FBRESET

Code de retour	Description
0	L'opération a réussi
-99	Erreur inconnue

## Codes de retour de l'instruction KAVSHELL DUMP

Tableau 115. Codes de retour de l'instruction KAVSHELL DUMP

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 indiqué en guise de chemin d'accès au dossier contenant le fichier dump est introuvable ; le processus avec le PID indiqué est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (tentative d'exécution de la commande KAVSHELL DUMP /OFF si la création des fichiers dump a déjà été désactivée)

Code de retour	Description
-99	Erreur inconnue

## Codes de retour de l'instruction KAVSHELL IMPORT

Tableau 116. Codes de retour de l'instruction 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)
-5	Syntaxe incorrecte
-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 Security for Windows Server n'a pas importé les paramètres d'un composant fonctionnel quelconque
-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 Security for Windows Server postérieure ou incompatible)

## Codes de retour de l'instruction KAVSHELL EXPORT

Tableau 117. Codes de retour de l'instruction 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

Code de retour	Description
501	L'opération a réussi, toutefois, pendant l'exécution de la commande, une erreur s'est produite, une remarque est affichée, par exemple, Kaspersky Security for Windows Server n'a pas exporté les paramètres d'un composant fonctionnel quelconque

# Contacteur le Support Technique

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

## Contenu du chapitre

Modes d'obtention de l'assistance technique .....	<a href="#">606</a>
Assistance technique via téléphone .....	<a href="#">606</a>
Assistance technique via Kaspersky CompanyAccount.....	<a href="#">607</a>
Utilisation du fichier de trace et du script AVZ.....	<a href="#">607</a>

## Modes d'obtention de l'assistance technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des sources d'informations relatives à l'application, contactez le Support Technique. Les employés du Support Technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Le Support Technique n'est pas proposé aux utilisateurs d'une version d'essai.

Avant de contacter le Support Technique, veuillez lire les règles d'octroi de l'assistance technique().

Voici comment contacter les experts du Support Technique de Kaspersky Lab :

- appeler le Support Technique par téléphone ;
- envoyer une requête au Support Technique de Kaspersky Lab via le portail Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

## Assistance technique via téléphone

Vous pouvez contacter les experts du Support Technique. depuis presque n'importe où dans le monde. Les informations sur la marche à suivre pour contacter le Support Technique dans votre région, y compris les coordonnées, sur le site Internet du Support Technique de Kaspersky Lab (<https://support.kaspersky.com/b2b>)

Avant de contacter le Support Technique, veuillez lire les règles d'octroi de l'assistance technique (<https://support.kaspersky.com/fr/support/rules>).

## Assistance technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) est un portail à disposition des entreprises qui utilisent les applications de Kaspersky Lab. Le portail Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky Lab via des requêtes électroniques. Le portail Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky Lab des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte utilisateur Kaspersky CompanyAccount. À l'aide d'un seul compte, vous pouvez centraliser l'administration des demandes électroniques envoyées par les employés à Kaspersky Lab et gérer les droits d'accès de ces employés à Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Vous pouvez également obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique ([http://support.kaspersky.com/fr/faq/companyaccount\\_help](http://support.kaspersky.com/fr/faq/companyaccount_help)).

## Utilisation du fichier de trace et du script AVZ

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Security for Windows Server à envoyer au Support Technique de Kaspersky Lab. Les experts du Support Technique de Kaspersky Lab peuvent également vous demander de créer un fichier de trace. Le fichier de trace permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

L'analyse des données que vous envoyez permet aux experts du Support technique de Kaspersky Lab de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus actifs, de rechercher la présence éventuelle de menaces sur l'ordinateur, de désinfecter ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse de l'ordinateur.

Pour une assistance plus efficace en cas de questions sur l'utilisation de l'application, les experts du Support Technique peuvent vous demander (pour la réparation) de modifier les paramètres de l'application pendant les diagnostics. Pour ce faire, l'exécution des actions suivantes peut être requise :

- Activer la fonctionnalité de traitement et stockage des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules séparés de l'application, qui n'est pas disponibles via les

outils standards de l'interface d'utilisateur.

- Modifier les paramètres de conservation et d'envoi des informations diagnostiques qui ont été traitées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

# Glossaire

## A

### Analyse heuristique

Technologie de détection des menaces dont les informations ne figurent pas encore dans les bases de Kaspersky Lab. L'analyse heuristique permet de détecter des objets dont le comportement dans le système d'exploitation peut constituer une menace pour la sécurité. Les objets identifiés à l'aide de l'analyse heuristique sont considérés comme probablement infectés. Par exemple, un objet qui contient une succession de commandes propres à des objets malveillants (ouverture d'un fichier, écriture dans le fichier) pourrait être considéré comme probablement infecté.

### Archive

Un ou plusieurs fichiers repris dans un fichier compressé. Une application dédiée, appelée archiveur, est requise pour le compactage et le décompactage des données.

## B

### Bases antivirus

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

## C

### Clé active

Clé actuellement utilisée par l'application.

## D

### Données relatives à la licence

Période de temps pendant laquelle vous avez accès aux fonctions de l'application et aux droits d'utiliser des services supplémentaires. Les services utilisables dépendent du type de licence.

### Désinfection

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être désinfectés.



## E

### Etat de la protection

Etat actuel de la protection, qui reflète le niveau de sécurité de l'ordinateur.

## F

### Faux positifs

Situation où un objet non infecté est considéré comme infecté par une application de Kaspersky Lab car son code évoque celui d'un virus.

### Fichier probablement infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'insertion de code malveillant est assez élevé pour ces fichiers.

## K

### Kaspersky Security Network (KSN)

Infrastructure de services cloud donnant accès à la base de données de Kaspersky Lab avec des informations constamment mises à jour sur la réputation des fichiers, les ressources Internet et le logiciel. Kaspersky Security Network assure une vitesse de réaction plus élevée que les applications de Kaspersky Lab face aux nouvelles menaces, augmente l'efficacité de certains composants de la protection et réduit la possibilité de faux positifs.

## M

### Masque de fichier

Représentation d'un nom de fichier à l'aide de caractères génériques. Les caractères génériques standard utilisés dans les masques de fichier sont \* et ?, où \* représente n'importe quel nombre de n'importe quels caractères et ? représente n'importe quel caractère unique.

### Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

## N

### Niveau d'importance de l'événement

Propriété d'un événement rencontré pendant le fonctionnement d'une application Kaspersky Lab. Gravité de l'événement : niveau de gravité de l'événement.

- Événement critique.
- Erreur.
- Avertissement
- Info.

Les événements du même type peuvent avoir différents niveaux de gravité en fonction de la situation de survenue de l'événement.

### Niveau de sécurité

Le niveau de sécurité est décrit comme un ensemble pré-configuré de paramètres de composants de l'application.

## O

### Objet OLE

Objet lié à un autre fichier ou imbriqué dans un autre fichier via la technologie Object Linking and Embedding (OLE). Exemple d'objet OLE : feuille de calcul Microsoft Office Excel® imbriquée dans un document Microsoft Office Word.

### Objets de démarrage

Ensemble d'applications nécessaires au démarrage et au fonctionnement corrects du système d'exploitation et au logiciel installé sur l'ordinateur. Objets de démarrage : objets que le système d'exploitation charge au démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

## P

### Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

### Protection en temps réel

Mode de fonctionnement de l'application sous lequel celle-ci analyse les objets pour y détecter la présence d'un code malveillant en temps réel.

L'application intercepte toutes les tentatives d'ouverture d'objet (lecture, écriture ou exécution) et analyse les objets pour y détecter les menaces. Les objets non infectés sont transmis à l'utilisateur ; les objets contenant des menaces ou les objets probablement infectés sont traités en fonction des paramètres de la tâche (désinfecté, supprimé ou en

quarantaine).

## Q

### Quarantaine

Dossier dans lequel l'application de Kaspersky Lab déplace les objets probablement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

## S

### Sauvegarde

Stockage spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur désinfection ou leur suppression.

### Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction de centralisation des informations relatives aux applications de Kaspersky Lab installées sur le réseau de la société et qui permet de les administrer. Il permet également de gérer ces applications.

### SIEM

Technologie qui analyse les événements de sécurité provenant de plusieurs périphériques réseau et applications.

### Stratégie

Une stratégie définit les paramètres d'une application et administre la possibilité de configurer cette application sur les ordinateurs au sein d'un groupe d'administration. Une stratégie individuelle doit être créée pour chaque application. Vous pouvez créer un nombre illimité de stratégies différentes pour les applications installées sur les ordinateurs dans chaque groupe d'administration mais une seule stratégie à la fois peut être appliquée à chaque application dans un groupe d'administration.

## T

### Tâche

Les fonctions de l'application de Kaspersky Lab sont mises en œuvre sous la forme de tâches, comme : Protection des fichiers en temps réel, Analyse complète de l'ordinateur et Mise à jour des bases de l'application.

### Tâche locale

Tâche définie et exécutée sur un ordinateur client unique.

## U

### Un objet infecté a été découvert

Objet dont une portion de code correspond parfaitement à une partie du code d'une application malveillante connue. Kaspersky Lab ne recommande pas d'accéder à ces objets.

## V

### Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs d'applications malveillantes pour pénétrer dans un système ou une application et nuire son intégrité. Un grand nombre de vulnérabilités dans un système rend son fonctionnement peu fiable car les virus, installés dans le système, peuvent entraîner des erreurs du système d'exploitation ou des applications installées.

# Kaspersky Lab

Kaspersky Lab est connu dans le monde entier pour ses systèmes de protection contre diverses menaces numériques telles que les virus et autres applications malveillantes, les emails indésirables (spams), les attaques de réseaux et les piratages.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie ("IDC Endpoint Tracker 2014").

Kaspersky Lab a été fondée en Russie en 1997. La société est devenue un groupe international qui compte 38 bureaux dans 33 pays. L'entreprise emploie plus de 3 000 experts qualifiés.

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

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des systèmes de contrôle industriel et la prévention des escroqueries financières. Ces solutions, associées à des outils d'administration centralisée, permettent de créer et d'exploiter une protection automatisée efficace de l'entreprise de n'importe quelle taille contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands laboratoires d'essai. Elles sont compatibles avec les logiciels de nombreux fournisseurs et sont optimisées pour une exécution sur de nombreuses plateformes.

Les experts antivirus de Kaspersky Lab travaillent 24 heures sur 24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et de désinfection de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab.

**Technologie.** De nombreuses technologies, sans lesquelles les antivirus actuels ne seraient pas ce qu'ils sont, ont justement été mises au point par Kaspersky Lab. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Antivirus a été adopté par de nombreux autres éditeurs de logiciels comme : Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu et ZyXEL. Beaucoup des innovations technologiques de l'entreprise sont brevetées.

**Résultats.** Au cours de ses années de lutte contre les menaces informatiques, Kaspersky Lab a remporté de nombreux prix. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais pour Kaspersky Lab, la plus grande récompense de toutes, c'est la fidélité des utilisateurs à travers le monde. Les produits et les technologies de la société assurent la protection de plus de 400 millions de particuliers et plus de 270 000 entreprises.

Site de Kaspersky Lab :	<a href="https://www.kaspersky.com/fr">https://www.kaspersky.com/fr</a>
Encyclopédie des virus :	<a href="https://securelist.com">https://securelist.com</a>
Kaspersky VirusDesk :	<a href="https://virusdesk.kaspersky.fr">https://virusdesk.kaspersky.fr</a> (pour l'analyse de fichiers ou de sites Internet suspects)
Communauté Internet de Kaspersky Lab :	<a href="https://community.kaspersky.com">https://community.kaspersky.com</a>

# Information sur le code tiers

Les informations sur le code tiers se trouvent dans le fichier legal\_notices.txt, situé dans le dossier d'installation de l'application.

# Avis de marques déposées

Les marques déposées et les marques de service appartiennent à leur propriétaire.

Citrix, XenApp et XenDesktop sont des marques de Citrix Systems, Inc. et/ou d'une ou plusieurs de ses filiales et peuvent être enregistrées au bureau des marques et brevets (Patent and Trademark Office) aux Etats-Unis et dans d'autres pays.

Dell et Dell Compellent sont des marques de Dell, Inc.

Dropbox est une marque de Dropbox, Inc.

EMC, Celerra, Isilon, OneFS et VNX sont des marques de commerce ou des marques déposées d'EMC Corporation aux Etats-Unis et/ou dans d'autres pays.

Hitachi est une marque de Hitachi, Ltd.

IBM et System Storage sont des marques d'International Business Machines Corporation déposées dans de nombreuses juridictions à travers le monde.

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

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server et Windows Vista sont des marques déposées de Microsoft Corporation aux Etats-Unis et dans d'autres pays.

NetApp and Data ONTAP sont des marques de commerce ou des marques déposées de NetApp, Inc. aux Etats-Unis et/ou dans d'autres pays.

Oracle est une marque déposée d'Oracle Corporation et/ou de ses filiales.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays, licenciée exclusivement via X/Open Company Limited.

# Index

## A

Action	
objet suspect .....	279
objets infectés .....	279
Actions à exécuter sur les objets .....	279, 302, 481
Analyse en cours	
durée maximale pour l'analyse d'un objet .....	279
niveau de sécurité .....	481
uniquement les objets neufs ou modifiés .....	279
Analyser les flux NTFS alternatifs.....	279
Archives .....	279

## B

Bases de données .....	178, 180
date de création.....	167
mise à jour automatique .....	158, 180, 184
mise à jour manuelle .....	184

## C

Configuration	
paramètres de sécurité.....	279, 480, 481
tâche.....	156, 184, 272, 302, 390, 397, 435, 440
Console de gestion .....	143, 151, 156
connexion .....	156
Démarrer .....	231
Contenu des mises à jour .....	188

## D

Désinfection d'objets.....	279
Dossier de sauvegarde.....	207
Dossier d'enregistrement des mises à jour.....	188



Dossier des journaux .....	221
Dossier pour la restauration	
Quarantaine.....	201

## E

Exclusions de la Zone d'analyse .....	279
---------------------------------------	-----

## F

Fenêtre principale de l'application .....	151
Fichier exécutable.....	279, 360, 390, 397, 400, 405
fichiers iSwift .....	195, 279, 481

## I

icône dans la zone de notification de la barre d'état .....	154
Interdire par défaut.....	415, 435
Interface de l'application .....	151
icône dans la zone de notification de la barre d'état .....	154

## J

Journal des événements.....	213, 220
-----------------------------	----------

## L

Lancement des tâches manquées.....	158
------------------------------------	-----

## M

Mise à jour	
modules de l'application .....	178
par planification .....	158, 184
Mode de protection .....	273

## P

Périphériques de confiance .....	415
----------------------------------	-----

Planification des tâches .....	158, 159
Protection en temps réel .....	286
Purge du journal d'audit système .....	216

## Q

Quarantaine	
consultation des objets .....	193, 194
restauration de l'objet .....	197
seuil d'espace disponible .....	201
suppression des objets.....	199
Quarantaine et Sauvegarde.....	193

## R

Recherche de virus dans les stockages .....	195
Règles .....	360, 416, 418, 420
contrôle des périphériques .....	416, 418, 420, 436, 437, 438, 439, 440
contrôle du lancement des applications .....	360, 390, 405, 408, 409, 410
Restauration de l'objet .....	197, 205
Restauration des paramètres par défaut .....	481

## S

Sauvegarde.....	203
configuration des paramètres.....	207
restauration d'objets en cours .....	205
suppression des objets.....	207
Serveur FTP.....	184, 188, 189
Serveur HTTP .....	180, 184, 188, 189
Serveur proxy.....	184
Source des mises à jour .....	184, 188, 189
Statistiques .....	167

## T

Tâche .....	156
-------------	-----

Taille maximale	
objet analysé .....	279
Quarantaine.....	201
Type de menace	
action .....	279