kaspersky

Kaspersky Endpoint Security for Linux 12.5.0

© 2026 AO Kaspersky Lab

Contenu

Kaspersky Endpoint Security for Linux
À propos de l'application
Principales fonctionnalités
Nouveautés de la version 12.5
Problèmes résolus
Configurations logicielles et matérielles
Distribution
Compatibilité avec d'autres applications
Comparaison des fonctionnalités des solutions Kaspersky
Déploiement et configuration initiale
Modes et schémas de déploiement
Préparation de l'environnement pour l'installation de l'application
Sélection du mécanisme d'interception des événements système
Préparation des paquets de distribution
Actions préparatoires dans Kaspersky Security Center
Installation de l'application à l'aide de Kaspersky Security Center
Installation de l'application à l'aide d'une ligne de commande
Étapes de configuration supplémentaires après l'installation dans certains systèmes d'exploitation
Scénario de migration vers Kaspersky Security Center for Linux à l'aide du script d'installation rapide
Mise à jour d'une ancienne version de l'application
À propos de la mise à jour des plug-ins de gestion de Kaspersky Endpoint Security
Paramètres de l'application après la mise à jour
Suppression d'une application
Utilisation de l'application
Licence
Comment passer à une autre solution Kaspersky
Gestion des clés de licence
Affichage des informations sur les clés de licence
Interfaces d'administration de l'application
Administration de l'application via Kaspersky Security Center
À propos des politiques de Kaspersky Security Center
Gestion des stratégies
Exportation et importation des paramètres d'une stratégie
À propos des tâches de Kaspersky Endpoint Security créées dans Kaspersky Security Center
Connexion et déconnexion de Web Console et de Cloud Console
Administrer l'application via la ligne de commande
Tâches locales de Kaspersky Endpoint Security
Modification des paramètres d'une tâche
Configuration de la planification des tâches
Gestion des paramètres généraux de l'application
Utilisation du filtre pour limiter les résultats des requêtes
Exportation et importation des paramètres de l'application
Administration de l'application via l'interface graphique

Surveillance de l'état de la protection
- États de la protection en temps réel
- Événements et rapports
  - Configuration d'enregistrement des événements dans le journal du système d'exploitation
  - Configuration des paramètres du journal des événements de l'application
  - Affichage des événements de l'application
  - Consulter les rapports
- Collecte de métriques d'état du système
- Surveillance de la stabilité des applications
- Vérification de l'intégrité des modules d'application

Contrôle de l'accès à l'application
- Rôles prédéfinis
- Comment attribuer ou révoquer un rôle utilisateur
- Zones fonctionnelles RBAC dans Kaspersky Security Center

Recommandations relatives aux rôles types des appareils protégés

Mise à jour des bases et des modules de l'application
- Comment sélectionner la source de mise à jour et le schéma de distribution
- Procédure de configuration de la tâche de mise à jour des bases de données
- Procédure de mise à jour à l'aide de Kaspersky Update Utility
- Procédure d'annulation des mises à jour des bases de données et des modules de l'application

Protection contre les menaces contre l'hôte
- Protection contre les fichiers malicieux
  - Comment créer une zone de protection
  - Comment sélectionner une action lors de la détection d'une menace dans un fichier
  - Qu'est-ce que le mode intelligent d'analyse des fichiers
  - Comment optimiser l'analyse des fichiers
  - Particularités de l'analyse des liens symboliques et matériels
- Analyse des logiciels malveillants
  - Comment créer une zone d'analyse
  - Comment configurer une planification d'analyse
  - Analyse d'un fichier ou d'un répertoire individuel
  - Optimisation des tâches d'analyse personnalisée
- Analyse des zones critiques
- Analyser les conteneurs
  - Configuration de l'intégration avec les outils de gestion des conteneurs
  - Création d'une zone d'analyse à la demande pour les conteneurs et les images
  - Comment optimiser l'Analyse du conteneur
  - Sélection de l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté
  - Exécution d'une analyse personnalisée des conteneurs et des images
- Analyse des disques amovibles
- Détection comportementale
- Protection contre les Exploits
- Protection contre le chiffrement
  - Comment sélectionner une action lors de la détection d'un chiffrement malveillant
  - Comment créer une zone de protection

- Protection BadUSB
  - Configuration de l'autorisation des appareils USB
  - Autorisation de la connexion d'appareils USB à l'aide du clavier visuel
  - Autorisation de la connexion d'appareils USB à l'aide du lecteur de codes-barres
- Protection des connexions réseau et des moyens de communications
  - Protection contre les menaces par emails
    - Que faire si une menace est détectée dans un email
    - Comment optimiser l'analyse des pièces jointes aux emails
    - À quoi sert un filtre des pièces jointes aux emails
  - Protection contre les menaces Internet
    - Comment sélectionner une action lors de la détection d'une menace Internet
    - Qu'est-ce que l'Antihameçonnage
  - Protection contre les menaces réseau
    - Comment sélectionner une action lors de la détection d'une menace réseau
    - Comment gérer les appareils bloqués
  - Gestion du pare-feu
    - Création d'une règle pour les paquets réseau
    - Exemples d'utilisation de règles pour les paquets réseau
    - Comment ajouter une adresse IP à une zone réseau : Publique, Locale, De confiance
    - Que sont les règles dynamiques
    - Comment créer des règles de connexion à Kaspersky Security Center
- Contrôles de sécurité
  - Contrôle des appareils
    - Administration de la liste des appareils de confiance à partir de la ligne de commande
    - Configuration du mode d'accès aux appareils
    - Comment configurer les règles d'accès aux appareils
    - Configuration du modèle de message du Contrôle des appareils
    - Autorisation d'accès temporaire à l'appareil
  - Contrôle Internet
    - Comment créer une règle d'accès aux ressources Internet
    - Comment modifier les modèles de messages du Contrôle Internet
    - Règles de formation des masques d'adresses de ressources Web
  - Contrôle des applications
    - Inventaire des applications
    - Comment configurer le mode de fonctionnement du Contrôle des applications
    - Création des catégories d'applications.
    - Image système
    - À propos des règles du contrôle des applications
    - Mode de test des règles du Contrôle des applications
  - Contrôle de l'intégrité du système
    - Surveillez l'intégrité du système en temps réel
    - Vérification de l'intégrité du système
- Exclusions de l'analyse pour l'application
  - Comment ajouter des exclusions de la protection
  - Comment ajouter des adresses Internet de confiance
  - Comment ajouter l'adresse IP de confiance d'un ordinateur
  - Comment sélectionner les ports réseau surveillés

- Comment ajouter un certificat à la liste des certificats racines de confiance
- Comment ajouter un domaine de confiance
- Comment exclure des points de montage
- Comment ajouter des applications de confiance
- Comment ajouter des appareils de confiance

Paramètres généraux

- Paramètres de détection
- Kaspersky Security Network
  - Comment activer ou désactiver Kaspersky Security Network
  - Qu'est-ce que le mode Cloud de l'application
  - À quoi sert le proxy KSN
- Configuration de l'envoi des informations vers le stockage de Kaspersky Security Center
- Comment configurer le lancement de l'application
- Configuration des autorisations de gestion des tâches
- Protection par mot de passe
  - À propos des autorisations personnalisées
  - Autorisations utilisateur par défaut
- Paramètres de performance
- Paramètres du réseau
  - Comment gérer les paramètres du proxy
  - Comment l'application intercepte le trafic
  - Configuration de la stratégie de validation des certificats
  - Configuration des ports surveillés
  - Exclusions à l'interception du trafic par le système d'exploitation
- Interception des opérations sur les fichiers
- Configuration des paramètres d'interception des événements système
- Configuration des paramètres avancés de la télémétrie
- Sauvegarde

Protection contre les menaces avancées et les attaques ciblées

- Actions de réponse
  - Trouver des indicateurs de compromission
  - Isolation réseau
    - Activer ou désactiver manuellement l'isolation réseau d'un appareil dans Web Console
    - Configuration de la durée d'isolement du réseau en mode automatique
    - Configuration des paramètres de l'isolation réseau en mode manuel
    - Configuration des exclusions de l'isolement du réseau dans Web Console
  - Mettre un fichier en quarantaine
  - Reception d'un fichier depuis un appareil
  - Suppression d'un fichier de votre appareil
  - Démarrage du processus
  - Terminer le processus
  - Prévention de l'exécution des objets
  - Travailler avec la quarantaine
- Endpoint Detection and Response Optimum
  - Comment activer l'intégration EDR Optimum
  - Comment vérifier que l'intégration d'EDR Optimum est opérationnelle
  - Cloud Sandbox

- Endpoint Detection and Response Expert (on-premises)
  - Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premises)
  - Comment configurer l'intégration d'EDR Expert (on-premises)
  - Comment vérifier que l'intégration EDR Expert (on-premises) est opérationnelle
- Endpoint Detection and Response Expert (cloud)
  - Comment configurer l'intégration de l'agent intégré avec EDR Expert (cloud)
  - Optimisation de la transmission des données de télémétrie d'EDR Expert (cloud)
  - Comment configurer les exclusions de télémétrie d'EDR Expert (cloud)
  - Comment exporter ou importer des filtres d'événements EDR Expert (cloud)
- Kaspersky Anti Targeted Attack Platform
  - Comment configurer l'intégration EDR (KATA)
  - Comment configurer l'intégration NDR (KATA)
  - Comment vérifier que l'Intégration KATA est opérationnelle
- Sandbox
  - Comment configurer l'intégration avec Sandbox
  - Comment vérifier que l'intégration avec Sandbox est opérationnelle
  - Comment envoyer manuellement un fichier à Sandbox
- Kaspersky Managed Detection and Response
  - Recommandations pour la création d'une image de référence en vue d'une intégration correcte avec MDR
  - Chargement du fichier de configuration KPSN
  - Comment configurer l'intégration MDR
  - Comment vérifier que l'intégration MDR est activée
- Kaspersky Unified Monitoring and Analysis Platform
  - Comment configurer l'intégration KUMA
  - Comment vérifier que l'Intégration KUMA est opérationnelle
- Protection des environnements virtuels
  - Comment configurer la découverte des SVM
  - Comment le Light Agent sélectionne les SVM
  - Comment équilibrer la connexion des Light Agents entre les SVM
  - Protection de la connexion entre le Light Agent et une SVM
  - Comment connaître l'état du Light Agent

Bonnes pratiques

- Optimisation de l'utilisation des ressources par l'application
  - Analyse du fonctionnement de l'application sur l'appareil
  - Recommandations pour la Protection contre les fichiers malicieux et les tâches d'analyse
  - Recommandations pour la Protection contre les menaces Internet et la Protection contre les menaces réseau
  - Recommandations pour la Détection comportementale
- Interopérabilité avec les solutions Kaspersky
  - Kaspersky Security Center Linux
  - Kaspersky Unified Monitoring and Analysis Platform

Référence des modules de l'application

- Commandes de gestion de Kaspersky Endpoint Security
  - Commandes de gestion des clés de licence
  - Commandes de gestion des utilisateurs et des rôles
  - Gestion des tâches et des paramètres de l'application
    - Commandes de gestion des paramètres généraux de l'application
    - Commandes de gestion des paramètres des tâches

- Commandes de gestion des tâches
- Commandes de gestion des paramètres généraux d'analyse du conteneur
- Commandes de gestion des paramètres d'analyse du trafic réseau
- Surveillance de l'état et de la protection
  - Commandes de statistiques
  - Commande d'affichage des événements
  - Commandes de gestion des événements de l'application
  - Commande de gestion des métriques de performance du système
- Contrôles de sécurité
  - Commandes de gestion du Contrôle des appareils
  - Commandes de gestion du Contrôle des applications
  - Commandes de gestion du Contrôle Internet
- Protection des connexions réseau
  - Commandes de contrôle pour les appareils bloqués
  - Commandes de gestion du pare-feu
- Protection contre les menaces avancées et les attaques ciblées
  - Commandes de gestion de la quarantaine
  - Commandes d'administration du module EDR Expert (on-premises)
  - Commandes d'administration du module Expert EDR (cloud)
  - Commandes d'administration des modules NDR (KATA)
  - Commandes de contrôle d'isolation réseau des appareils
  - Commandes de gestion des paramètres d'intégration avec KUMA
  - Commandes de gestion des paramètres d'intégration avec Sandbox
  - Commandes de gestion de l'analyse IOC
- Commandes de l'application en mode Light Agent

Options de ligne de commande de l'application

- Tâche de mise à jour
- Protection contre les menaces contre l'hôte
  - Tâche Protection contre les fichiers malicieux
  - Optimisation de la vérification des répertoires réseau
  - Analyse des logiciels malveillants
    - Tâche d'analyse des logiciels malveillants
    - Tâche d'analyse personnalisée
  - Tâche d'analyse des zones critiques
  - Tâche d'analyse des disques amovibles
  - Analyser les conteneurs
    - Paramètres d'analyse de conteneur
    - Tâche Analyse du conteneur
    - Intégration à Jenkins
  - Tâche Protection contre le chiffrement
  - Tâche Détection comportementale
  - Protection contre les Exploits
  - Utilisation de Kaspersky Security Network
    - Connexion à Kaspersky Security Network
    - Activation ou désactivation du mode Cloud
  - Tâche Protection BadUSB

Protection des connexions réseau et des moyens de communications
Tâche de protection contre les menaces Internet
Analyse du trafic réseau
Affichage et modification des paramètres de vérification du trafic réseau
Affichage des exclusions liées à l'analyse des connexions chiffrées
Gestion de la liste des certificats racines de confiance
Configuration et affichage des exclusions à l'interception du trafic
Tâche de protection contre les menaces réseau
Gestion du pare-feu
Configuration de la liste des règles pour les paquets réseau
Configuration des zones réseau
Contrôles de sécurité
Tâche Contrôle des appareils
Contrôle Internet
Tâche Contrôle Internet
Affichage et modification des paramètres de contrôle Internet
Contrôle des applications
Tâche Contrôle des applications
Créer et modifier une liste des catégories
Consultation de la liste des catégories
Configuration de la liste des règles du Contrôle des applications
Configuration de l'inventaire
Tâche Inventaire
Consultation de la liste des applications détectées
Tâche Contrôle de l'intégrité du système
Tâche Vérification de l'intégrité du système
Protection contre les menaces avancées et les attaques ciblées
Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)
Paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)
Gestion des certificats de connexion aux serveurs OSMP EDR Expert (on-premises)
Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)
Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)
Gestion des certificats de connexion aux serveurs OSMP EDR Expert (cloud)
Intégration à Kaspersky Endpoint Detection and Response (KATA)
Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)
Gestion des certificats pour la connexion au serveur KATA
Intégration avec Kaspersky Network Detection and Response (KATA)
Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)
Gestion des certificats pour la connexion au serveur NDR
Intégration avec Sandbox
Paramètres d'intégration avec Sandbox
Gestion des certificats pour la connexion au serveur Sandbox
Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum
Configuration de l'intégration de Kaspersky Managed Detection and Response
Administration de l'isolation réseau des appareils
Configuration des paramètres de la quarantaine
Travailler avec des fichiers de quarantaine dans la ligne de commande

- Trouver des indicateurs de compromission
- Gestion de la prévention de l'exécution
- Configuration de l'intégration KUMA
  - Tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform
  - Gestion des certificats pour la connexion au serveur KUMA
- Paramètres généraux
  - Paramètres généraux de l'application
  - Planification de la tâche
  - Configuration du serveur proxy
  - Configuration des paramètres de la sauvegarde
  - Paramètres d'analyse du trafic réseau
  - Configuration des exclusions globales
  - Paramètres de la Protection par mot de passe
- Paramètres de l'application dans la Console d'administration
  - Mise à jour des bases de l'application
  - Protection contre les menaces contre l'hôte
    - Protection contre les fichiers malicieux
      - Fenêtre Zones d'analyse
      - Fenêtre Nouvelle zone d'analyse
      - Fenêtre Paramètres d'analyse
      - Fenêtre Actions en cas de détection d'une menace
      - Exclusions de la Protection contre les fichiers malicieux
        - Fenêtre Zones d'exclusion
        - Fenêtre Nouvelle zone d'exclusion
        - Fenêtre Exclusions d'après le masque
        - Fenêtre Exclusions d'après le nom de la menace
        - Fenêtre Exclusions par processus
        - Fenêtre Processus de confiance
    - Analyse des logiciels malveillants
      - Fenêtre Zones d'analyse
      - Fenêtre <Nouvelle zone d'analyse>
      - Fenêtre Paramètres de la zone d'analyse
      - Fenêtre Zones d'analyse
      - Fenêtre Paramètres d'analyse
      - Fenêtre Actions en cas de détection d'une menace
      - Section Exclusions
      - Fenêtre Zones d'exclusion
      - Fenêtre Nouvelle zone d'exclusion
      - Fenêtre Exclusions d'après le masque
      - Fenêtre Exclusions d'après le nom de la menace
    - Analyse des zones critiques
      - Fenêtre Zones d'analyse
      - Fenêtre Nouvelle zone d'analyse
      - Fenêtre Paramètres de la zone d'analyse
      - Fenêtre Zones d'analyse
      - Fenêtre Paramètres d'analyse
      - Fenêtre Actions en cas de détection d'une menace

- Section Exclusions
- Fenêtre Zones d'exclusion
- Fenêtre Nouvelle zone d'exclusion
- Fenêtre Exclusions d'après le masque
- Fenêtre Exclusions d'après le nom de la menace
- Surveillance des conteneurs
  - Fenêtre Paramètres d'analyse de conteneur
- Analyser les conteneurs
  - Fenêtre Paramètres d'analyse de conteneur
  - Fenêtre Paramètres d'analyse
  - Fenêtre Actions en cas de détection d'une menace
  - Section Exclusions
  - Fenêtre Exclusions d'après le masque
  - Fenêtre Exclusions d'après le nom de la menace
- Analyse des disques amovibles
- Détection comportementale
  - Fenêtre Exclusions par processus
  - Fenêtre Processus de confiance
- Protection contre les Exploits
  - Fenêtre Exclusions de la Protection contre les Exploits
  - Fenêtre Exclusion de la Protection contre les Exploits
- Protection contre le chiffrement
  - Fenêtre Zones d'analyse
  - Fenêtre Nouvelle zone d'analyse
  - Fenêtre Paramètres de la protection
  - Fenêtre Zones d'exclusion
  - Fenêtre Nouvelle zone d'exclusion
  - Fenêtre Exclusions d'après le masque
- Kaspersky Security Network
  - Paramètres de Kaspersky Security Network
  - Déclaration de Kaspersky Security Network
  - Déclaration de Kaspersky Private Security Network
- Protection BadUSB

Protection des connexions réseau et des moyens de communications

- Protection contre les menaces par emails
  - Fenêtre Paramètres de la protection contre les menaces par emails
  - Fenêtre Filtre des pièces jointes
- Protection contre les menaces Internet
  - Fenêtre Adresses Internet de confiance
  - Fenêtre Paramètres d'analyse
- Protection contre les menaces réseau
  - Fenêtre Exclusions
- Gestion du pare-feu
  - Fenêtre Règles de paquet réseau
  - Fenêtre Ajout d'une règle de paquet réseau
  - Fenêtre Ajout d'adresses IP

- Fenêtre Réseaux disponibles
- Fenêtre Connexion réseau

Contrôles de sécurité

- Contrôle des appareils
  - Fenêtre Appareils de confiance
  - Fenêtre Appareil de confiance (ID de l'appareil)
  - Fenêtre Appareils sur les appareils clients
  - Fenêtre Liste des appareils en fonction des événements du Contrôle des appareils
  - Fenêtre Accès à un appareil de confiance
  - Fenêtre Utilisateur ou groupe
  - Fenêtre Type d'appareil
  - Fenêtre Configuration de la règle d'accès aux appareils
  - Fenêtre Utilisateur ou groupe
  - Fenêtre Planification d'accès
  - Fenêtre Bus de connexion
- Contrôle Internet
  - Fenêtre Règle du Contrôle Internet
  - Fenêtre Sélectionner les catégories de contenu
  - Fenêtre Sélectionner les catégories de type de données
  - Fenêtre Sélectionner les adresses
  - Fenêtre Sélectionner un groupe d'adresses
  - Fenêtre Ajout d'un groupe d'adresses
  - Fenêtre Sélectionner les utilisateurs
  - Fenêtre Utilisateur ou groupe
  - Fenêtre Planification d'accès
- Contrôle des applications
  - Fenêtre Règles du Contrôle des applications
  - Fenêtre Ajouter une nouvelle règle
  - Fenêtre Catégories d'applications
  - Fenêtre Utilisateur ou groupe
  - Inventaire
    - Fenêtre Zones d'analyse
    - Fenêtre Nouvelle zone d'analyse
    - Section Exclusions
    - Fenêtre Zones d'exclusion
    - Fenêtre Nouvelle zone d'exclusion
- Contrôle de l'intégrité du système
  - Fenêtre Zones d'analyse
  - Fenêtre Nouvelle zone d'analyse
  - Fenêtre Zones d'exclusion
  - Fenêtre Nouvelle zone d'exclusion
  - Fenêtre Exclusions d'après le masque
  - Vérification de l'intégrité du système
    - Fenêtre Zones d'analyse
    - Fenêtre Nouvelle zone d'analyse
    - Section Exclusions
    - Fenêtre Zones d'exclusion

Fenêtre Nouvelle zone d'exclusion
Fenêtre Exclusions d'après le masque
Tâches locales
Gestion de la tâche
Protection contre les menaces avancées et les attaques ciblées
Intégration avec la solution Kaspersky Managed Detection and Response
Intégration de Kaspersky Endpoint Detection and Response (on-premises)
Configuration de connexion aux serveurs KATA
+-/Configuration des paramètres généraux de connexion aux serveurs KATA
Configuration des paramètres du transfert des données aux serveurs KATA
Intégration avec Kaspersky Network Detection and Response (KATA)
Configuration de connexion aux serveurs NDR
+-/Configuration des paramètres généraux de connexion aux serveurs NDR
Configuration des paramètres du transfert des données aux serveurs NDR
Intégration avec KUMA
Fenêtre Serveurs KUMA
Fenêtre Serveur KUMA
Fenêtre Paramètres de connexion aux serveurs KUMA
Fenêtre d'ajout d'un certificat de serveur
Fenêtre d'ajout d'un certificat client
Quarantaine
Prévention de l'exécution des objets
Paramètres généraux
Serveur Proxy
Fenêtre Exclusions pour le serveur proxy
Utilisation du processeur par les tâches d'analyse
Exécution de tâches sur batterie
Lancement de l'application
Redémarrage automatique à la réception d'une mise à jour critique
Protection par mot de passe
Paramètres de traçage et d'enregistrement de vidage
Utilisation de la mémoire résidente par l'application
Analyse des connexions chiffrées
Fenêtre Domaines de confiance
Fenêtre Certificats de confiance
Fenêtre Exclusions de l'interception du trafic
Fenêtre Exclusion de l'interception du trafic
Fenêtre Ports contrôlés
Exclusions globales
Fenêtre Chemin du point de montage
Exclure la mémoire de processus de l'analyse
Sauvegarde
Détection des applications que les intrus peuvent utiliser pour causer des dommages
Interception des opérations sur les fichiers
Envoi d'informations vers le stockage de Kaspersky Security Center
Interception des événements système
Paramètres avancés de collecte de télémétrie

- Mode Light Agent
  - Connexion au serveur d'intégration
    - Fenêtre Connexion au serveur d'intégration
    - Fenêtre Vérification du certificat du Serveur d'intégration
    - Fenêtre Authentification sur le Serveur d'intégration
  - Paramètres de détection des SVM
  - Tag de connexion à la SVM
  - Algorithme de sélection des SVM
  - Protection de la connexion
- Problèmes connus et limitations
- Contacter le Support technique
  - Support technique via le Kaspersky CompanyAccount
  - Obtention d'informations pour le Support technique
    - Comment activer et configurer la création de fichiers de traçage
    - Activation et configuration de l'enregistrement des vidages
  - Diagnostic à distance de l'appareil à l'aide de Kaspersky Security Center
- Annexes
  - Annexe 1. Fichiers de configuration et paramètres de l'application par défaut
    - Règles d'édition des fichiers de configuration des tâches de l'application
    - Fichiers de configuration initiale
    - Paramètres de configuration initiale dans le paquet d'installation
    - Fichiers de configuration préinstallés
    - Paramètres des tâches de ligne de commande par défaut
      - Paramètres par défaut de la tâche File_Threat_Protection (ID:1)
      - Paramètres par défaut de la tâche Scan_My_Computer (ID:2)
      - Paramètres par défaut de la tâche Scan_File (ID:3)
      - Paramètres par défaut de la tâche Critical_Areas_Scan (ID:4)
      - Paramètres par défaut pour la tâche Update (ID:6)
      - Paramètres par défaut de la tâche System_Integrity_Monitoring (ID:11)
      - Paramètres par défaut de la tâche Firewall_Management (ID:12)
      - Paramètres par défaut de la tâche Anti_Cryptor (ID:13)
      - Paramètres par défaut de la tâche Web_Threat_Protection (ID:14)
      - Paramètres par défaut de la tâche Device_Control (ID:15)
      - Paramètres par défaut de la tâche Removable_Drives_Scan (ID:16)
      - Paramètres par défaut de la tâche Network_Threat_Protection (ID:17)
      - Paramètres par défaut pour les tâches Container_Scan (ID:18) et Custom_Container_Scan (ID:19)
      - Paramètres par défaut de la tâche Behavior_Detection (ID:20)
      - Paramètres par défaut de la tâche Application_Control (ID:21)
      - Paramètres par défaut de la tâche Inventory_Scan (ID:22)
      - Paramètres par défaut de la tâche KATAEDR (ID:24)
      - Paramètres par défaut pour la tâche Web_Control (ID:26)
      - Paramètres par défaut de la tâche Standalone_Sandbox (ID:29)
      - Paramètres par défaut de la tâche KATANDR (ID:31)
      - Paramètres par défaut de la tâche KUMA (ID:33)
      - Paramètres par défaut de la tâche Protection contre les menaces par emails (ID : 35)
      - Paramètres par défaut de la tâche Protection BadUSB (ID:37)
      - Paramètres par défaut de la tâche KATANDR (ID:31)

Annexe 2. Configuration de la collaboration avec Kaspersky Antivirus for Linux Mail Server
Annexe 3. Paramètres d'interaction avec les services externes
Annexe 4. Extensions de fichiers pour l'analyse rapide des disques amovibles
Annexe 5. Variables dans les modèles de messages
Annexe 6. Événements relatifs aux applications
Critique
Avertissement
Messages d'information
Annexe 7. Codes de retour
Annexe 8. Préparation d'une archive contenant les bases de données de l'application
Annexe 9. Exigences pour les fichiers IOC
Mentions légales
À propos des données
Données fournies lors de l'utilisation d'un code d'activation
Données fournies lors du téléchargement des mises à jour depuis les serveurs de mise à jour de Kaspersky
Données transférées lors de l'utilisation de l'application en mode Light Agent
Données transmises à l'application Kaspersky Security Center
Données fournies lorsque vous cliquez sur des liens depuis l'interface de l'application
Données fournies lors de l'utilisation de Kaspersky Security Network
Données fournies lors de l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum
Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response (KATA)
Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response Expert (on-premises)
Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response Expert (cloud)
Données fournies lors de l'intégration avec Kaspersky Network Detection and Response (KATA)
Données fournies lors de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform
Informations sur le code tiers
Notice sur les marques de commerce

Kaspersky Endpoint Security for Linux

Parcourir

Kaspersky Endpoint Security for Linux
Nouveautés de la version 12.5
Schémas de déploiement types
Comparaison des fonctionnalités
Problèmes connus et limitations

Démarrage rapide

Configurations logicielle et matérielle
Compatibilité
Préparation des paquets de distribution
Préparation de l'environnement pour l'installation
Déploiement de l'application
Scénario de migration vers Kaspersky Security Center Linux

Utilisation de l'application

Activation
Mise à jour des bases de données
Mise à jour à l'aide de Kaspersky Update Utility
Protection contre les fichiers malicieux
Zone de confiance
Optimisation des ressources

Configuration sur la ligne de commande

Administrer l'application via la ligne de commande
Commandes de gestion
Options de ligne de commande de l'application

Support technique

Surveillance de l'état de la protection
Mise à jour à partir de la version précédente de l'application
Contacter le Support technique

À propos de l'application

Kaspersky Endpoint Security for Linux offre une protection avancée et complète des appareils Linux et permet de prévenir, détecter et traiter différents types de menaces, d'attaques réseau et de fraudes. L'application est incluse dans de nombreuses solutions multiplateformes de Kaspersky et peut être configurée de manière flexible pour répondre aux défis de l'infrastructure informatique de votre organisation.

Vous pouvez administrer Kaspersky Endpoint Security installé sur les appareils protégés localement ainsi que de manière centralisée à l'aide de Kaspersky Security Center.

L'application n'est pas destinée à être utilisée dans des processus technologiques utilisant des systèmes de gestion automatisés. Pour protéger les appareils de tels systèmes, il est recommandé d'utiliser l'application Kaspersky Industrial CyberSecurity for Linux Nodes.

Principales fonctionnalités

Protection contre les cybermenaces de masse

La protection basée sur des technologies avancées constitue le fondement de votre sécurité informatique. Kaspersky Endpoint Security empêche l'infection des systèmes de fichiers des appareils des utilisateurs, surveille la connexion des disques amovibles à l'appareil et les analyse à la recherche de virus. Il surveille l'activité malveillante des applications et protège les fichiers contre le chiffrement à distance malveillant. Les bases de données contenant des informations sur les nouvelles menaces mondiales, par exemple les virus, les chevaux de Troie, les chiffreurs et les attaques de pirates informatiques, sont mises à jour régulièrement et automatiquement.

Communication et protection Internet

Kaspersky Endpoint Security protège de manière fiable l'environnement réseau de votre organisation : il analyse les emails, les sites Internet et les fichiers téléchargés à la recherche de virus, de vers réseau et d'autres menaces avant que vous ne les ouvriez. L'application permet d'analyser le trafic réseau entrant à la recherche d'une activité pouvant indiquer une attaque réseau, surveille les paramètres du pare-feu du système d'exploitation et filtre l'activité réseau.

Contrôles de sécurité du poste de travail

En utilisant Kaspersky Endpoint Security pour contrôler l'accès des utilisateurs aux applications, aux ressources Internet et aux appareils connectés sur le poste de travail, vous fournissez une couche de sécurité supplémentaire à votre organisation. Cela permet de protéger les appareils contre l'infection et de prévenir la perte ou les fuites de données.

Protection contre les menaces avancées et les attaques ciblées

L'application peut interagir avec les solutions Kaspersky Detection and Response, à savoir Kaspersky Managed Detection and Response (MDR) et Kaspersky Anti Targeted Attack Platform (KATA). La solution SIEM de Kaspersky, Kaspersky Unified Monitoring and Analysis Platform (KUMA), est également prise en charge. Kaspersky Endpoint Security surveille les processus en cours d'exécution sur les appareils des utilisateurs, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. L'interaction avec les solutions Detection and Response assure une protection contre les menaces telles que les exploits, les ransomwares, les attaques sans fichier et les outils système légitimes que les pirates informatiques peuvent utiliser pour compromettre les appareils ou les données.

Protection des environnements virtuels et cloud

Kaspersky Endpoint Security, dans le cadre de la solution Kaspersky Security for Virtualization Light Agent, assure la protection des machines virtuelles exécutant des systèmes d'exploitation invités Linux sur diverses plateformes de virtualisation de serveurs et plateformes VDI. L'analyse des objets à la recherche de virus est effectuée par un module spécial installé sur une machine virtuelle distincte, la SVM (Secure Virtual Machine). Ainsi, l'application assure la sécurité en utilisant les ressources de la SVM au lieu de celles de la machine virtuelle, ce qui, avec l'optimisation intelligente (par exemple, l'utilisation d'un cache partagé), minimise la charge globale sur l'infrastructure informatique.

Nouveautés de la version 12.5

Kaspersky Endpoint Security 12.5 for Linux introduit les fonctionnalités et améliorations suivantes :

- Prise en charge de l'installation de Kaspersky Endpoint Security 12.5 for Linux sur les appareils équipés de processeurs Elbrus. L'application offre une prise en charge limitée des processeurs Elbrus.

- L'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) a été mise en œuvre. Cette solution cloud est conçue pour protéger l'infrastructure informatique de l'organisation contre les cybermenaces avancées, y compris celles qui ne peuvent pas être détectées par les applications EPP installées sur les actifs de l'entreprise. La solution offre une visibilité, une corrélation et une automatisation complètes en exploitant un large éventail d'outils de réponse et de sources de données, notamment les actifs des terminaux, les données réseau et les données de l'environnement cloud, ce qui permet un processus unifié de Detection and Response grâce à des modules intégrés et à des workflows de bout en bout au sein d'une interface unique afin d'améliorer l'efficacité des spécialistes de la sécurité.

  > L'intégration de Kaspersky Endpoint Security for Linux avec la solution Kaspersky Endpoint Detection and Response Expert (cloud) n'est temporairement pas disponible jusqu'au lancement de cette solution, prévu fin 2026. Après cela, l'intégration devrait devenir disponible pour cette version de Kaspersky Endpoint Security sans nécessiter de mises à jour supplémentaires.

- Protection par mot de passe de certaines actions dans l'application Kaspersky Endpoint Security. La protection par mot de passe permet de restreindre les actions que les utilisateurs peuvent effectuer avec l'application Kaspersky Endpoint Security conformément aux autorisations qui leur ont été accordées. La restriction de l'accès aux paramètres de l'application réduit le risque de modifications non autorisées ou involontaires de l'application.

- Amélioration du module Contrôle des appareils. Vous pouvez désormais exporter la liste des appareils de confiance vers un fichier et l'importer depuis un fichier.

- Amélioration du module Protection BadUSB. Désormais, lorsque vous connectez un lecteur de codes-barres, vous pouvez scanner un code-barres affiché à l'écran pour autoriser le lecteur au lieu de saisir un code d'autorisation afin de déverrouiller l'appareil.

- Améliorations apportées au module de noyau mis à jour (ULKM) :
  - Ajout de la prise en charge de l'interception des événements système basée sur le module de noyau mis à jour (ULKM) pour les systèmes sur lesquels Secure Boot est activé.
  - L'application prend désormais en charge davantage de systèmes d'exploitation sur lesquels le module de noyau mis à jour peut être utilisé pour intercepter des événements.
  - Nous avons ajouté la prise en charge du module de noyau mis à jour pour les modules Protection contre le chiffrement et Contrôle des appareils.
- Le processus d'installation en mode d'environnement logiciel fermé d'Astra Linux Special Edition a été amélioré Désormais, si un pack de compatibilité est installé, l'utilisateur n'a pas besoin d'effectuer manuellement des actions supplémentaires pour lancer l'application Kaspersky Endpoint Security après l'avoir installée sur un appareil doté du système d'exploitation Astra Linux Special Edition.
- Désormais, lors de l'installation de l'application, vous pouvez modifier les paramètres du fichier de configuration kesl.ini à l'aide du fichier de configuration autoinstall.ini.
- Amélioration du diagnostic des erreurs lors de l'installation et de la désinstallation de l'application :
  - Les codes de retour sont désormais plus détaillés pour faciliter la compréhension des éventuels problèmes.
  - Nouveaux messages relatifs aux dépendances manquantes (bibliothèques externes, modules, utilitaires ou autres programmes) nécessaires à l'installation et au bon fonctionnement de l'application.
  - Nouveaux messages relatifs aux autorisations d'accès mal configurées des répertoires système.
  - Kaspersky Security Center affiche des messages d'erreur nouveaux et clarifiés.
  - Vous pouvez désormais ignorer les erreurs du gestionnaire de paquets lors de l'installation de l'application.
- Le redémarrage automatique de l'application a été mis en place lorsque des mises à jour critiques sont reçues lors de la première mise à jour des bases de données et des modules dans les 24 heures suivant l'installation de l'application.
- Vous pouvez désormais configurer l'application pour qu'elle redémarre automatiquement à la réception de mises à jour critiques. Vous pouvez configurer le redémarrage automatique de l'application dans les propriétés de la stratégie à l'aide de Web Console ou de la Console d'administration, ou en ligne de commande dans les paramètres généraux de l'application.
- Désormais, lors de l'intégration avec des solutions Detection and Response, vous pouvez gérer le cache des événements à l'aide du paramètre `UseIncreasedXdrEventsCache` dans le fichier de configuration kesl.ini. Il existe un compromis entre performances élevées et consommation de RAM.
- Désormais, vous pouvez effectuer un arrêt rapide du processus kesl lors de l'arrêt ou du redémarrage de l'application à l'aide du paramètre `FastShutdown` dans le fichier de configuration kesl.ini, ce qui permet de réduire au minimum le temps d'arrêt de l'application sur les systèmes à forte charge et d'éviter une consommation excessive des ressources.
- Vous pouvez désormais limiter la consommation de mémoire du module Analyse comportementale pour le traitement de la file d'attente des événements à l'aide du paramètre `ReduceSWMemoryConsumption` du fichier de configuration kesl.ini. L'utilisation de ce paramètre peut avoir une incidence sur le niveau de protection. Veillez à consulter la documentation.

- Amélioration de la stabilité de l'accès au réseau. Désormais, si le processus kesl se termine de manière anormale, le serveur Watchdog supprime les règles de pare-feu que l'application ajoute au lancement des modules Protection contre les menaces Internet et Protection contre les menaces réseau, ce qui vous permet d'éviter de perdre la connexion Internet et de restaurer rapidement l'accès au réseau sur l'appareil.

- Vous pouvez désormais empêcher l'exécution simultanée de plusieurs tâches d'analyse afin d'optimiser les performances de l'application. Lorsque cette option est activée, plusieurs tâches d'analyse lancées simultanément sont mises en file d'attente.

- Les exclusions de Protection contre les fichiers malicieux peuvent désormais traiter les liens symboliques. Les chemins d'accès sont désormais convertis en adresses finales des fichiers.

- Vous pouvez désormais activer et configurer le répertoire des fichiers de vidage à l'aide de la commande de gestion des paramètres généraux de l'application, sans redémarrer l'application. Ces paramètres de configuration des fichiers de vidage ont été supprimés du fichier de configuration kesl.ini.

- Un mot de passe est désormais obligatoire lors de l'intégration avec les solutions Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform et Kaspersky Unified Monitoring and Analysis Platform. Désormais, lors de la configuration de l'intégration, vous devez spécifier un mot de passe pour le certificat client.

- L'application peut désormais compresser le trafic lors de l'envoi d'événements de télémétrie dans le cadre de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform, ce qui permet d'économiser de la bande passante.

- La liste des systèmes d'exploitation pris en charge a été mise à jour, notamment avec la prise en charge des versions 64 bits de CentOS 5.2, 5.4, 6.4 et 6.6.

- L'interface de l'application est disponible dans de nouvelles langues : espagnol (Mexique) et portugais (Brésil).

Modifications dans les versions antérieures

Version 12.4

Kaspersky Embedded Systems Security 12.4 for Linux présente désormais les nouvelles fonctionnalités et améliorations suivantes :

- * Un nouveau module fonctionnel Protection contre les menaces par emails a été ajouté. Ce module analyse les pièces jointes des messages entrants et sortants à la recherche de virus et autres pièces jointes malveillantes.

- * Un nouveau module fonctionnel Protection BadUSB a été ajouté. Le module empêche la connexion des appareils USB infectés imitant des claviers à l'appareil client.

- Amélioration du module Contrôle des appareils. Il est désormais possible d'accorder un accès temporaire aux appareils bloqués à la demande de l'utilisateur.

- Le module Protection contre les Exploits a été amélioré. Vous pouvez désormais configurer des exclusions d'analyse spécifiques aux modules pour les objets.

- Le module de noyau mis à jour a été amélioré.

  - Le module de noyau mis à jour vous permet désormais d'optimiser l'interception des opérations sur les fichiers. Les performances de l'application sont améliorées grâce à l'utilisation d'un cache de fichiers et de processus ne nécessitant pas de vérification.

  - Avec le module de noyau mis à jour, vous pouvez désormais affiner les exclusions globales. Si le mécanisme d'interception basé sur fanotify est utilisé, les points de montage spécifiés sont entièrement exclus de l'interception des opérations sur les fichiers. Le module de noyau mis à jour vous permet d'exclure des répertoires locaux ou distants spécifiques montés sur l'appareil.

- Le module EDR (KATA), qui assure l'intégration avec Kaspersky Endpoint Detection and Response (KATA), a été renommé EDR Expert (on-premises). Ce module fournit également la tâche Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises). La tâche d'intégration a été renommée *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* (KATAEDR, ID : 24).

- Vous pouvez désormais configurer l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), une solution de cybersécurité d'entreprise qui permet de se défendre contre la plupart des risques de cybersécurité et de couvrir les principaux scénarios de propagation des menaces. Les modules de Kaspersky Endpoint Detection and Response Expert (on-premises) sont déployés sur la plateforme de gestion unique Open Single Management Platform (OSMP). L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) prend en charge toutes les fonctionnalités de l'Intégration de Kaspersky Endpoint Detection and Response (KATA), ainsi que de nouvelles fonctionnalités :

  - Lancement de l'analyse YARA. Une *analyse YARA* est un processus au cours duquel Kaspersky Endpoint Security utilise des fichiers YARA pour rechercher des signatures d'activités malveillantes sur l'appareil.

  - Collecte de données forensiques : données numériques pouvant servir de preuves dans le cadre d'enquêtes sur des incidents liés à la cybercriminalité et aux fuites de données.

  - Envoi des données d'événements étendues (télémétrie) au serveur de collecte de télémétrie sur OSMP.

  - Envoi des données de télémétrie uniquement avec un indicateur d'attaque (Indicator of Attack, IOA). Vous pouvez désormais configurer des filtres personnalisés dans la stratégie de Web Console.

  - Activation du module EDR Expert (on-premises), qui permet l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) et avec Kaspersky Endpoint Detection and Response (KATA), par l'ajout d'une clé de licence.

  - Sélection d'un mode d'intégration dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* via la ligne de commande ou dans les propriétés de la stratégie dans Web Console.

- L'application peut désormais être utilisée en mode Endpoint Detection and Response Agent, les solutions Detection and Response de Kaspersky et les applications antivirus tierces peuvent fonctionner conjointement sur les appareils protégés. Dans ce mode, les modules de protection et de contrôle standards de Kaspersky Endpoint Security ne sont pas utilisés pour protéger l'appareil. La protection standard de l'appareil est alors assurée par une application tierce.

- Ajout de la possibilité de créer des fichiers de traçage de l'application lors du premier lancement après l'installation. Vous pouvez désormais activer la création de fichiers de traçage lors du premier lancement de l'application dans Web Console, la Console d'administration ou dans le fichier de configuration d'installation initiale.

- L'interface de la stratégie dans Web Console a été mise à jour. La structure des sections de la stratégie a été remaniée afin de trouver plus rapidement les fonctions dont vous avez besoin.

- Vous pouvez désormais sélectionner le mode d'interception du trafic : la technologie eBPF ou l'utilitaire iptables.
- Ajout de la possibilité de sélectionner une source de télémétrie (eBPF uniquement ou eBPF et auditd). Pour auditd, vous pouvez également sélectionner le mode de fonctionnement (mode exclusif ou mode multicast).
- Désormais, vous pouvez sélectionner le mode d'envoi des fichiers et des répertoires vers la sandbox pour analyse : manuel, automatique uniquement, automatique et manuel.
- Les fonctionnalités de l'application ont été étendues lors de l'utilisation en mode Light Agent :
  - Un mécanisme d'interception des événements système basé sur le module de noyau mis à jour est disponible.
  - Le module fonctionne Prévention des Exploits est disponible.
  - Le niveau de détection des menaces est amélioré.
- Ajout de la possibilité d'utiliser Kaspersky Private Security Network (KPSN) directement, sans passer par le service proxy KSN sur le Serveur d'administration.
- Il est désormais possible de créer des stratégies pour les utilisateurs autonomes dans la Web Console et la Console d'administration. Ces stratégies sont appliquées lorsque l'appareil quitte le réseau d'organisation.
- Lors de l'affichage et de l'exportation de la liste des points de montage dans Web Console et dans la Console d'administration, ainsi que lors de leur affichage dans la ligne de commande, des informations indiquent désormais que le point de montage a été détecté dans l'espace de noms.
- Ajout d'un mécanisme alternatif pour recevoir la télémétrie système dans le module Détection comportementale sur les systèmes d'exploitation 64 bits avec la version du noyau 4.18 et supérieure avec prise en charge d'eBPF, qui vous permet de libérer les ressources du sous-système d'audit du noyau auditd.
- Ajout de la possibilité d'inclure les informations suivantes dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response :
  - indicateur précisant que l'événement s'est produit dans un conteneur ;
  - identifiant de l'espace de noms du conteneur ;
  - nom du conteneur.
- La liste des systèmes d'exploitation pris en charge a été mise à jour.

Version 12.3

Kaspersky Embedded Systems Security 12.3 for Linux présente désormais les nouvelles fonctionnalités et améliorations suivantes :

- Ajout d'un mécanisme d'interception des événements système basé sur le module de noyau mis à jour (non disponible en mode Light Agent). Si le système d'exploitation de votre appareil prend en charge fanotify et répond à d'autres exigences pour l'installation d'un module de noyau mis à jour, vous pouvez configurer l'utilisation du module de noyau mis à jour dans l'application. L'utilisation du module noyau mis à jour vous permet d'optimiser l'interception des processus démarrés par Kaspersky Endpoint Security. Le module de noyau mis à jour est inclus avec l'application.
- Le module de noyau mis à jour améliore le fonctionnement du module Protection contre le chiffrement (non disponible en mode Light Agent). L'application peut désormais détecter davantage de types de ransomwares.

- Ajout d'un nouveau module fonctionnel : Protection contre les Exploits (non disponible en mode Light Agent). Le module surveille le code logiciel qui utilise les vulnérabilités de l'appareil pour obtenir des privilèges d'administrateur par l'Exploit ou effectuer des actions malveillantes.

- Amélioration du module Contrôle des appareils :

  - Ajout de la possibilité de configurer une liste d'utilisateurs ou de groupes d'utilisateurs pour lesquels les appareils ajoutés seront approuvés.

  - Ajout de la possibilité d'autoriser l'accès en lecture seule aux appareils de stockage.

  - Nous avons également amélioré la notification des utilisateurs par le biais d'événements, en ajoutant de nouveaux événements et en clarifiant et systématisant les textes des événements dans les plug-ins et sur la ligne de commande.

- Extension des possibilité d'intégration avec la solution Kaspersky Managed Detection and Response :

  - Implémentation de la possibilité d'isoler l'appareil du réseau.

  - Implémentation de la possibilité de mettre des fichiers en quarantaine et de restaurer des fichiers depuis la quarantaine.

  - Implémentation de la possibilité de démarrer et de terminer un processus.

- Nous avons ajouté la possibilité d'activer le module MDR, qui assure l'intégration avec Kaspersky Managed Detection and Response, en ajoutant une clé de licence.

- Le module Détection comportementale a été amélioré. Ajout de la possibilité de configuration de l'exclusion d'un processus de l'analyse lorsque les modules MDR et EDR (KATA) sont en cours d'exécution.

- Implémentation de la possibilité de configurer des exclusions lors de l'utilisation d'un serveur proxy. Vous pouvez désormais spécifier les modules de l'application Kaspersky Endpoint Security qui n'utiliseront pas de serveur proxy et également créer une liste d'adresses auxquelles un serveur proxy ne sera pas utilisé pour les connexions. Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation d'un serveur proxy pour se connecter à Kaspersky Security Network, SVM et Serveur d'intégration n'est pas prise en charge.

- Ajout de la possibilité de configurer des exclusions à l'interception du trafic. Vous pouvez désormais utiliser les plug-ins d'administration de l'application ou la ligne de commande pour spécifier les connexions que l'application doit exclure de l'interception du trafic.

- Ajout de la possibilité d'exclure temporairement les fichiers journaux de base de données de l'analyse pour optimiser leur analyse par la Protection contre les fichiers malicieux. Si un fichier journal de base de données est réutilisé par le même processus dans les 10 minutes suivant la dernière vérification, l'application ne vérifiera pas ce fichier journal.

- Implémentation de la possibilité d'activer la fusion des éléments de la liste d'exclusion dans les stratégies parent et enfant lors de l'héritage des paramètres de stratégie parent.

- La possibilité d'exporter et d'importer des listes d'exclusion dans les stratégies et les tâches a été ajoutée au plug-in Web d'administration des applications.

- Ajout de la possibilité de configurer les paramètres de configuration initiale de l'application Kaspersky Endpoint Security dans la Console d'administration de Kaspersky Security Center lors de la création d'un paquet d'installation ou dans les propriétés du paquet d'installation.

- Ajout de la possibilité de configurer l'annulation des tâches planifiées sur un appareil fonctionnant sur batterie.
- Implémentation de la possibilité d'activer et de désactiver l'utilisation du serveur proxy KSN lorsque l'application Kaspersky Endpoint Security interagit avec les serveurs KSN (non disponible en mode Light Agent). Si l'utilisation du serveur proxy KSN est activée, Kaspersky Endpoint Security communique avec les serveurs KSN à l'aide du service du serveur proxy KSN sur le Serveur d'administration. Si l'utilisation du serveur proxy KSN est désactivée, Kaspersky Endpoint Security communique directement avec les serveurs KSN.
- Dans la ligne de commande, vous pouvez utiliser une commande qui affiche la liste des fonctions de l'application, des informations sur leur état (utilisées ou non) et les technologies Linux avec lesquelles ces fonctions de l'application sont implémentées.
- Ajout de la possibilité d'afficher des informations sur la stratégie et les profils de stratégie actuellement en vigueur sur l'appareil dans la ligne de commande et dans l'interface graphique.
- Implémentation de la possibilité d'installer l'application à l'aide de la ligne de commande sur un appareil qui ne dispose pas d'un interpréteur de langage Perl.
- Interception du trafic améliorée. Désormais, le trafic local (trafic entre les processus situés sur le même appareil) n'est pas intercepté.
- Implémentation de la possibilité de transférer les paramètres nécessaires à l'envoi de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response sans utiliser le fichier de configuration KPSN. Si vous utilisez la solution d'infrastructure Kaspersky Security Network ou si vous ne disposez que d'un locataire racine, le fichier de configuration KPSN n'est pas requis pour l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Managed Detection and Response.
- Stockage optimisé d'un grand nombre d'événements dans le journal des événements de l'application. L'ouverture et la fermeture de la base de données d'événements, ainsi que la récupération des événements, sont désormais des opérations plus rapides.
- Nous avons amélioré l'interface graphique de l'application (si l'application est utilisée en mode Light Agent, l'interface graphique n'est pas prise en charge) :
  - Vous pouvez désormais activer ou désactiver le module Contrôle Internet.
  - Le style de l'interface graphique a été repensé (les couleurs ont été modifiées, des coins arrondis ont été ajoutés à toutes les fenêtres).
- Les noms des actions sur les objets infectés dans les paramètres de la Protection contre les fichiers malicieux et les tâches d'analyse ont été modifiés.
- L'ajout d'un mécanisme alternatif pour recevoir la télémétrie système dans le module Détection comportementale sur les systèmes d'exploitation 64 bits avec la version du noyau 5.3 et supérieure avec prise en charge d'eBPF, qui vous permet de libérer les ressources du sous-système d'audit du noyau auditd. Si le système d'exploitation satisfait aux exigences, l'application utilise également automatiquement eBPF en mode Light Agent.
- L'affichage de la date et de l'heure dans toutes les interfaces de gestion des applications (à l'exception de la ligne de commande) a été ramené à un format unique défini dans la RFC 3339, tel que 2023-12-25 23:55:59.
- La liste des systèmes d'exploitation pris en charge a été mise à jour.

Version 12.2

Kaspersky Embedded Systems Security 12.2 for Linux présente désormais les nouvelles fonctionnalités et améliorations suivantes :

- La possibilité d'intégration avec Kaspersky Network Detection and Response (KATA) (module de la solution Kaspersky Anti Targeted Attack Platform) a été mise en œuvre, ce qui garantit la protection du réseau interne de l'entreprise et vous permet d'envoyer des données sur les événements sur les appareils (télémétrie) au serveur Kaspersky Anti Targeted Attack Platform avec le module Central Node (ci-après également serveur NDR).

- La possibilité d'intégration avec KATA Sandbox (module de la solution Kaspersky Anti Targeted Attack Platform) a été mise en œuvre, ce qui vous permet d'analyser et d'analyser des objets pour identifier les activités malveillantes et les signes d'attaques ciblées sur l'infrastructure informatique de l'entreprise sur des serveurs spéciaux avec des images virtuelles déployées des systèmes d'exploitation.

- La possibilité d'intégration avec Kaspersky Unified Monitoring and Analysis Platform (solution logicielle complète) a été mise en œuvre, qui combine les fonctionnalités suivantes : réception, traitement et stockage des événements de sécurité des informations ; analyse et corrélation des données entrantes ; recherche des événements reçus et création des notifications sur l'identification des signes de menaces pour la sécurité informatique.

- Les possibilités d'intégration avec Kaspersky Endpoint Detection and Response (KATA), un module de la solution Kaspersky Anti Targeted Attack Platform, ont été étendues :

  - La fonctionnalité de prévention du lancement des objets a été implémentée.

  - La possibilité de mettre les fichiers en quarantaine a été implémentée.

  - Les données sur les événements sur les appareils (télémétrie) ont été étendues.

- Les possibilités d'intégration avec la solution Endpoint Detection and Response Optimum ont été étendues :

  - La fonctionnalité de prévention du lancement des objets a été implémentée.

  - La possibilité de mettre les fichiers en quarantaine a été implémentée.

  - La possibilité d'exclure un processus de l'isolation réseau par son nom a été implémentée.

- Ajout de la possibilité d'utiliser la technologie Cloud Sandbox, qui vous permet de détecter des menaces complexes sur votre appareil. Kaspersky Endpoint Security envoie automatiquement les fichiers détectés à Cloud Sandbox pour analyse. Cloud Sandbox exécute ces fichiers dans un environnement isolé pour détecter les activités malveillantes et prend des décisions concernant la réputation de ces fichiers.

- Implémentation de la possibilité d'afficher des statistiques sur les fichiers et les applications les plus fréquemment analysés, ainsi qu'une liste des points de montage détectés sur l'appareil protégé. Pour améliorer les performances, vous pouvez désormais exclure les fichiers les plus fréquemment analysés par le module Protection contre les fichiers malicieux, les chemins d'accès aux applications les plus fréquemment analysés par le module Détection comportementale et les points de montage détectés sur l'appareil.

- Ajout de la possibilité de collecter des métriques liées aux performances des applications et vous permettre d'analyser l'impact de l'application Kaspersky Endpoint Security sur le système d'exploitation.

- Le module Gestion du pare-feu a été amélioré. Ajout de la possibilité de spécifier plusieurs adresses IP ou plages d'adresses IP pour une règle de paquet réseau.

- Ajout d'un mécanisme de suivi des blocages du système d'exploitation. Le mécanisme vérifie le blocage de certaines fonctions du système, l'une de ces fonctions est la fonction execve. Le processus de surveillance wdserver démarre un autre processus wdserver toutes les trois secondes, dans lequel il appelle ces fonctions système (l'appel de la fonction execve démarre au moins un autre processus wdserver). Si wdserver détecte une fonction système qui ne répond pas, la surcharge du serveur Watchdog redémarre le processus kesl.

- Ajout de la possibilité de configurer l'affichage des notifications contextuelles lors de l'utilisation de l'interface utilisateur graphique de l'application. Vous pouvez désormais activer ou désactiver l'affichage des notifications contextuelles dans l'interface graphique à l'aide de la Web Console, de la Console d'administration ou de la ligne de commande.

- Amélioration des paramètres de planification des tâches dans la ligne de commande. Vous pouvez désormais configurer une tâche pour qu'elle s'arrête lorsqu'elle atteint la durée d'exécution maximale autorisée.

- L'état des attributs « cadenas » a été modifié lors de la création d'un profil de la stratégie de Kaspersky Security Center. Désormais, lors de la création d'un profil par défaut, tous les « cadenas » sont ouverts afin que, par défaut, les paramètres du profil ne remplacent pas les paramètres de la stratégie « de base ».

- Ajout d'un mécanisme alternatif pour recevoir la télémétrie système sur les systèmes d'exploitation 64 bits (avec la version du noyau 5.3 et supérieure avec prise en charge d'eBPF avec BTF), qui vous permet de libérer les ressources du sous-système d'audit du noyau auditd. L'application fonctionnera automatiquement avec eBPF si le système d'exploitation répond aux exigences spécifiées.

- L'affichage de la date et de l'heure dans tous les plug-ins de gestion des applications a été ramené à un format unique défini dans la RFC 3339, tel que 2023-12-25 23:55:59.

- La liste des systèmes d'exploitation pris en charge a été mise à jour.

Version 12.1

Kaspersky Embedded Systems Security 12.1 for Linux présente désormais les nouvelles fonctionnalités et améliorations suivantes :

- Vous pouvez désormais configurer l'intégration avec Kaspersky Endpoint Detection and Response Optimum, qui protège l'infrastructure informatique de l'organisation contre les menaces telles que les exploits, les ransomwares, les attaques sans fichier et l'utilisation par les attaquants d'outils système légitimes pour nuire aux appareils ou aux données.

- Il est désormais possible d'ajouter deux clés de licence actives à l'application : une clé primaire pour activer l'application et une clé supplémentaire pour activer la fonctionnalité Kaspersky Endpoint Detection and Response Optimum. Une clé supplémentaire est requise si votre licence principale n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum.

- Un nouveau module fonctionnel *Contrôle Internet* a été ajouté, qui contrôle l'accès des utilisateurs aux ressources Web. Cela vous permet de réduire la consommation de trafic et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur tente d'ouvrir un site dont l'accès est restreint par le Contrôle Internet, l'application Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement.

- Une fonction de surveillance de la stabilité de Kaspersky Endpoint Security a été implémentée, qui vous permet de suivre le nombre d'arrêts anormaux de l'application et d'informer l'administrateur du fonctionnement instable de l'application.

- La procédure d'installation de Kaspersky Endpoint Security à l'aide de Kaspersky Security Center Web Console a été améliorée : dans les propriétés du paquet d'installation de l'application, vous pouvez désormais spécifier les paramètres initiaux de l'application qui n'étaient auparavant disponibles que dans le fichier de configuration autoinstall.ini.

- La possibilité de gérer des paramètres supplémentaires de l'application via Kaspersky Security Center Web Console et la Console d'administration de Kaspersky Security Center a été étendue : vous pouvez configurer des paramètres qui ne pouvaient auparavant être configurés qu'en modifiant le fichier de configuration kesl.ini.

- Ajout de la possibilité d'activer ou de désactiver l'utilisation d'exclusions globales et d'exclusions de la Protection contre les menaces sur les fichiers lors de l'exécution de tâches d'analyse.

- La possibilité d'intégration avec Kaspersky Symphony XDR a été implémentée : si l'application Kaspersky Endpoint Security est utilisée en mode standard, l'application peut effectuer les actions de réponse « Analyse des logiciels malveillants » et « Mettre à jour les bases ».

- Vous pouvez désormais envoyer des informations sur tous les appareils installés ou connectés aux appareils clients (y compris ceux installés et connectés précédemment mais actuellement déconnectés) au Serveur d'administration lorsque l'application est gérée à l'aide de Kaspersky Security Center.

- Les règles d'interception du trafic ont été améliorées pour prendre en charge l'interaction des conteneurs sur le même réseau.

- La liste des systèmes d'exploitation pris en charge a été mise à jour.

Problèmes résolus

Le tableau ci-dessous répertorie tous les problèmes découverts dans les versions précédentes de Kaspersky Endpoint Security et corrigés dans la version actuelle.

Liste des problèmes corrigés dans la version 12.5

Identifiant	Description
10306343	Lors de la vérification de l'état de la clé de licence actuelle, des notifications relatives à la suppression et à l'installation d'une clé de licence étaient générées à tort.
10295949	Les paramètres spécifiés dans le profil de stratégie actuel pour le module Contrôle des appareils n'étaient pas appliqués. Par conséquent, le module continuait à fonctionner avec les paramètres spécifiés dans la stratégie.
10171454	Si la première source de mise à jour spécifiée dans les paramètres était indisponible, un message signalant un problème de mise à jour s'affichait à tort.
10109293	Si le mode d'interception du trafic réseau iptables était sélectionné (`NetInterceptorMode=UseIPTables`), le trafic des applications ouvrant des sockets réseau associés à une interface réseau spécifique était traité de manière incorrecte.
10024219	La Console d'administration de Kaspersky Security Center affichait de manière incorrecte l'état du module de noyau mis à jour sur les appareils administrés.
9995631	La limitation de l'utilisation de la mémoire RAM résidente par l'application (paramètre `MaxMemory`) ne fonctionnait pas correctement sur les systèmes sans partition d'échange. Désormais, lorsque la limite définie est atteinte, Kaspersky Endpoint Security redémarre.
9937329	*Appareil connecté* et *Appareil déconnecté* étaient générés à tort sur les systèmes où la tâche Contrôle des appareils (Device_Control) était désactivée.
9934846	L'application ne démarrait pas sur les systèmes soumis à une charge élevée. Le délai d'expiration de la connexion de l'application au serveur Watchdog a été augmenté.
9846405	Des événements *Objet non traité* étaient générés à tort sur les systèmes dotés d'un chargeur d'amorçage EFI configuré.
9815051	Les connexions réseau précédemment établies pouvaient se bloquer lors de l'exécution des tâches Protection contre les menaces Internet (Web_Threat_Protection) et Protection contre les menaces réseau (Network_Threat_Protection) sur les appareils administrés en mode d'interception du trafic réseau eBPF (`NetInterceptorMode=UseEBPF`). Ces connexions sont désormais interrompues lors d'une tentative de transmission de données.
9807202	Sur certains systèmes d'exploitation ROSA, des problèmes d'installation survenaient lors de l'utilisation de l'utilitaire mkfs.ext2.

Identifiant	Description
9704644	L'état de l'appareil s'affichait de manière incorrecte lorsque l'application était utilisée en mode agent EDR. La valeur de l'état de protection de l'appareil lorsque l'application est utilisée en mode Endpoint Detection and Response Agent a été modifiée.
9643969	Dans certains cas, lors de l'utilisation de l'interception du trafic réseau en mode eBPF, un problème de connectivité réseau peut survenir entre les hôtes Scylla.
9633030	Le problème lié au démarrage de la tâche Prévention de l'exécution pour les objets (EDR Expert (on-premises)) lorsque la case **Activer la prévention de l'exécution pour les objets** est décochée dans la stratégie a été corrigé.
9627894	Le mode d'interception du trafic réseau basé sur la technologie eBPF a été corrigé sur les systèmes d'exploitation sur lesquels IPv6 est désactivé.
9606448	Un problème survenait lors de l'activation de l'application à l'aide du Serveur d'administration de Kaspersky Security Center en tant que serveur proxy pour accéder aux serveurs d'activation de Kaspersky (lorsque la case **Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation** était cochée dans la stratégie).
9508605	Lorsque l'intégration de Kaspersky Endpoint Detection and Response Expert était activée, l'application utilisait une grande quantité de mémoire sur les systèmes dotés d'un environnement de conteneurs.
9456741	L'application se bloquait en raison de l'impossibilité de déterminer l'interpréteur du fichier lors de l'interception du démarrage d'un nouveau processus.

Liste des problèmes corrigés dans le plug-in web 12.5.0.7391

Identifiant	Description
9558745	Le paramètre **Afficher les notifications contextuelles dans l'interface utilisateur graphique** permettant de configurer l'affichage des notifications dans l'interface graphique de Kaspersky Endpoint Security ne s'affichait pas dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Paramètres des événements → Paramètres avancés**).
9622658	Lors de l'ajout d'exclusions de l'Analyse des logiciels malveillants selon le hachage de l'objet, ces exclusions n'étaient pas enregistrées.
9798821	Lors de l'ajout d'un site particulier à une règle de Contrôle Internet, les modifications de la stratégie n'étaient pas enregistrées.
9990129	Un champ **Commentaire** non pertinent s'affichait dans le formulaire d'ajout d'une application de confiance.
9977884	Un bouton bascule **Niveau de sécurité** non pertinent s'affichait dans les paramètres du module Protection contre les menaces par emails.
9944635	Le nom des indicateurs **Analyser les bases de messagerie** était dupliqué. Les noms corrects s'affichent désormais : **Analyser les bases de messagerie** et **Analyser les fichiers au format de messagerie**.
10010439	Lors de la création de règles de Contrôle Internet, l'utilisateur affecté à la règle à partir de la liste Active Directory était ajouté de manière incorrecte.
10218308	Le mode Kaspersky Security Network était réinitialisé lorsque les paramètres de la stratégie étaient modifiés.

Configurations logicielles et matérielles

Configuration matérielle minimale requise

Pour l'installation de l'application

- Un processeur doté d'une architecture AMD64, de 2 GHz ou plus, comportant deux cœurs ou plus et prenant en charge les instructions SSE2.
- Espace d'échange d'au moins 1 Go

- mémoire vive :
  - Pour les systèmes d'exploitation 64 bits : 2 Go de RAM disponibles pour l'application
  - Pour les systèmes d'exploitation 32 bits : 1 Go de RAM disponible pour l'application
- 4 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;

  Un espace disque supplémentaire est nécessaire pour stocker les fichiers de traçage de l'application et les fichiers de vidage de l'application.

  Lors de l'analyse des archives et des objets composés, la Protection contre les fichiers malicieux et les tâches d'analyse nécessitent également un espace disque supplémentaire, dont la quantité dépend du type et de la taille décompressée de ces objets lorsque les paramètres `ScanArchived=Yes` et/ou `ScanSfxArchived=Yes` sont définis (par défaut, ces paramètres sont définis sur `Yes` pour les tâches d'analyse et sur `No` pour la Protection contre les fichiers malicieux).

  Il est recommandé de prévoir suffisamment d'espace dans le répertoire /tmp pour analyser les archives et les objets composés. Vous pouvez également limiter la taille des archives analysées (décompressées) à l'aide du paramètre `SizeLimit` pour chaque tâche.

Pour installer l'interface graphique

- Un moniteur capable d'afficher des fenêtres de 1 000 pixels de large sur 600 pixels de haut. Si la mise à l'échelle de l'écran est appliquée, ces dimensions sont également mises à l'échelle.

Configuration matérielle minimale requise pour l'architecture Arm

Pour l'installation de l'application

- Processeur Armv8.2-A Kunpeng 920 ou Armv8-A Baikal-M (BE-M1000) ou la plateforme terminal m-TrusT.
- un secteur de pagination d'au moins 1 Go ;
- 2 Go de RAM disponibles pour l'application.
- 3 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;

  Un espace disque supplémentaire est nécessaire pour stocker les fichiers de traçage de l'application et les fichiers de vidage de l'application.

  Lors de l'analyse des archives et des objets composés, la Protection contre les fichiers malicieux et les tâches d'analyse nécessitent également un espace disque supplémentaire, dont la quantité dépend du type et de la taille décompressée de ces objets lorsque les paramètres `ScanArchived=Yes` et/ou `ScanSfxArchived=Yes` sont définis (par défaut, ces paramètres sont définis sur `Yes` pour les tâches d'analyse et sur `No` pour la Protection contre les fichiers malicieux).

  Il est recommandé de prévoir suffisamment d'espace dans le répertoire /tmp pour analyser les archives et les objets composés. Vous pouvez également limiter la taille des archives analysées (décompressées) à l'aide du paramètre `SizeLimit` pour chaque tâche.

Pour installer l'interface graphique

- Un moniteur capable d'afficher des fenêtres de 1 000 pixels de large sur 600 pixels de haut. Si la mise à l'échelle de l'écran est appliquée, ces dimensions sont également mises à l'échelle.

Configuration matérielle minimale requise pour l'architecture Elbrus (E2K)

Pour l'installation de l'application

- Processeur v3 : Elbrus-4S ; v4 : Elbrus-8S ou Elbrus-1S+
- Partition d'échange d'au moins 2 Go
- 2 Go de RAM disponibles pour l'application.
- 2 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux

Pour installer l'interface graphique

- Un moniteur capable d'afficher des fenêtres de 1 000 pixels de large sur 600 pixels de haut. Si la mise à l'échelle de l'écran est appliquée, ces dimensions sont également mises à l'échelle.

Configuration logicielle

Pour installer Kaspersky Endpoint Security, l'un des systèmes d'exploitation répertoriés dans le tableau doit être installé sur l'appareil :

Cet article répertorie les versions des logiciels sur lesquelles l'application a été testée et avec lesquelles son bon fonctionnement est garanti. L'application peut également fonctionner avec d'autres versions de logiciels, mais ces configurations n'ont pas fait l'objet d'un cycle de test complet et ne figurent pas dans la liste des versions dont la prise en charge est garantie.

En raison des limitations techniques, l'application fanotify ne prend pas en charge les systèmes de fichiers suivants : autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

La Protection contre les fichiers malicieux pour les points de montage via la technologie FUSE est limitée en l'absence d'étapes supplémentaires que l'administrateur du système d'exploitation doit effectuer. Vous pouvez ajouter le paramètre user_allow_other au fichier /etc/fuse.conf et l'option de montage allow_root pour chaque point de montage, ce qui permet à l'application de surveiller les événements liés aux fichiers sur ces points de montage.

Systèmes d'exploitation 64 bits	Systèmes d'exploitation 64 bits pour l'architecture Arm	Systèmes d'exploitation 64 bits pour l'architecture Elbrus (E2K)	Systèmes d'exploitation 32 bits
• AlmaLinux OS 8.6, 8.7, 8.8, 8.9 • AlmaLinux OS 9.4, 9.5, 9.6 • AlterOS® 2025. • Amazon™ Linux 2023. • Astra Linux Common Edition 2.12. • Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.5, 1.6, 1.7, 1.8). • Astra Linux Special Edition RUSB.10015-03 (operational update 7.6) • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6). • Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3). • Astra Linux Special Edition RUSB.10015-37 (operational update 7.7) Le système d'exploitation Astra Linux en mode « Mobile » est pris en charge uniquement en mode bureau. • CentOS 5.2, 5.4, 6.4, 6.6, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. Dans la solution Kaspersky Endpoint Security Cloud, l'application ne prend pas en charge l'exécution sur les appareils CentOS 5.2, 5.4, 6.4 et 6.6. Dans Kaspersky Security Center Cloud Console, l'application ne prend pas en charge l'exécution sur les appareils CentOS 5.2, 5.4, 6.4 et 6.6. • CentOS Stream 8, 9, 10. • Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13. • Debian GNU/Linux 13.1, 13.2, 13.3 • EMIAS 1.0. • EulerOS 2.0 SP10. • Fedora Linux 41. • Kylin Desktop OS V10 SP1. • Linux Mint 21.3 • Linux Mint 22.2 • Mostech 12 release 2021.1 • openSUSE Leap 15.6 • Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 • Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9 • Oracle Linux 9.4, 9.5, 9.6 • Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 • Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10. • Red Hat Enterprise Linux 9.4, 9.5, 9.6 • Red Hat Enterprise Linux 10.0, 10.1 • Rocky Linux 8.6, 8.7, 8.8, 8.9 • Rocky Linux 9.4, 9.5, 9.6 • SberLinux 8.10, 9.1, 9.5, 9.6, 9.7. • SberOS 3.4.0, 3.5.0, 3.6.1. • SUSE Linux Enterprise Server 12.5, 12.6, 12.7 • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 • Ubuntu® 24.04 LTS. • Ubuntu 26.04 LTS. • ALT Éducation 10, 11. • ALT Workstation 11. • ALT Server 11 • ALT SP Workstation version 10. • ALT SP Server version 10. • Atlant, version Alcyone, 2022.02. • GosLinux 7.2. • M OS 12 Server version 2021.1.	• Astra Linux Special Edition RUSB.10152-02 (operational update 4.7) • CentOS Stream 9 • EulerOS 2.0 SP10. • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 • Ubuntu 26.04 LTS. • ALT Workstation 11.2 • ALT Server 11.1 • ALT SP Workstation version 10. • ALT SP Server version 10. • RED OS 8.0	• OS Elbrus 9.3.6. • Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1). • Astra Linux Special Edition RUSB.10265-01 (operational update 8.1) • ALT SP Workstation version 8, 10. • ALT SP Server version 8, 10.	• Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13.

Systèmes d'exploitation 64 bits	Systèmes d'exploitation 64 bits pour l'architecture Arm	Systèmes d'exploitation 64 bits pour l'architecture Elbrus (E2K)	Systèmes d'exploitation 32 bits
• MOS OS 15.5 Arbat • MSVSphere 9.5 Workstation. • SERVEUR MSVSPHERE 9.5 Server • OS MESH 12 Pour les écoles de Moscou pour panneaux interactifs (avec télémétrie et support DIT) release 2025 • OS MESH 12 pour les écoles de Moscou pour ordinateurs et ordinateurs portables (avec télémétrie et support DIT) release 2025 • OSnova 3.1. • RED OS® 7.3. • RED OS 8.0 • ROSA « Cobalt » 7.9 Workstation. • ROSA « Cobalt » 7.9 Server. • ROSA « Chrome » 12 Workstation. • ROSA « Chrome » 12 Server. • ROSA 13.1. • SynthesisM-Client 8.6. • SynthesisM-Serveur 8.6.			

Configuration logicielle et matérielle supplémentaire requise pour le mode Light Agent

L'application Kaspersky Endpoint Security peut être utilisé comme Light Agent dans le cadre de Kaspersky Security for Virtualization Light Agent version 6.5. Vous pouvez consulter les exigences relatives aux infrastructures virtuelles pour exécuter l'application en mode Light Agent dans l'aide de Kaspersky Security for Virtualization Light Agent.

Machines virtuelles

Les exigences logicielles et matérielles de Kaspersky Endpoint Security s'appliquent, avec les limitations suivantes, aux machines virtuelles sur lesquelles Kaspersky Endpoint Security est installé en mode Light Agent :

- Une interface réseau virtualisée avec une bande passante de 100 Mbit/s est nécessaire
- Sur les appareils Arm, Kaspersky Endpoint Security en mode Light Agent n'est pas pris en charge.
- L'application en mode Light Agent n'est pas prise en charge dans les systèmes d'exploitation Astra Linux Special Edition en mode de contrôle d'accès obligatoire et en mode d'environnement logiciel fermé.

Le BIOS d'une machine virtuelle doit prendre en charge la spécification SMBIOS version 2.1 ou ultérieure.

Selon votre infrastructure virtuelle, les éléments suivants doivent être installés sur les machines virtuelles :

- Dans une infrastructure Microsoft Hyper-V, le paquet Integration Services.
- Dans une infrastructure VMware vSphere, le paquet VMware Tools.
- Dans une infrastructure XenServer, le logiciel XenTools.
- Dans une infrastructure HUAWEI FusionSphere, le paquet HUAWEI Tools.
- Dans une infrastructure KVM (Kernel-based Virtual Machine), QEMU Guest Agent.

Types de serveurs de terminaux pris en charge

- Serveur de terminaux Astra Linux 3.0.5.

Distribution

Le paquet de l'application Kaspersky Endpoint Security comprend les fichiers suivants :

Fichiers principaux de l'application

- Pour les processeurs avec système d'exploitation 32 bits :
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- Pour les processeurs avec système d'exploitation 64 bits :
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- Pour les processeurs Arm® avec système d'exploitation 64 bits :
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- Pour le processeur Elbrus :
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

Interface graphique de l'application

- Pour les processeurs avec système d'exploitation 32 bits :
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- Pour les processeurs avec système d'exploitation 64 bits :
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- Pour les processeurs Arm® avec système d'exploitation 64 bits :
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- Pour le processeur Elbrus :
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

Pour installer l'application Kaspersky Endpoint Security sur des systèmes d'exploitation à prise en charge limitée (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), sélectionnez le paquet de distribution portant la mention `OLD`.

Archive pour l'installation à distance de l'application à l'aide de Kaspersky Security Center

`kesl-12.5.0.<build number>.zip`

L'archive contient également les textes des contrats utilisateur.

Textes des contrats utilisateur

- `ksn_license.<language ID>` contient le texte de la Déclaration de Kaspersky Security Network.
- `license.<language ID>` contient le texte du Contrat de licence utilisateur final. Le Contrat de licence utilisateur final indique les conditions dans le cadre desquelles vous pouvez utiliser l'application.

L'Agent d'administration de Kaspersky Security Center n'est pas inclus dans le paquet. Vous pouvez le télécharger depuis la page de téléchargement des applications dans la section **Kaspersky Security Center**.

Compatibilité avec d'autres applications

Versions prises en charge de Kaspersky Security Center

Selon le mode de Kaspersky Endpoint Security, vous pouvez administrer l'application à l'aide des versions de Kaspersky Security Center indiquées dans le tableau.

Mode	Version de Kaspersky Security Center
Kaspersky Endpoint Security en mode standard	Kaspersky Security Center Windows 14.2, 15.1. Administration via la Console d'administration à l'aide du plug-in d'administration MMC et via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web. Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2, 16.3. Administration via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web.
Kaspersky Endpoint Security en mode standard avec le module Endpoint Detection and Response Optimum	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.
Kaspersky Endpoint Security en mode Light Agent	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 16.1, 16.2, 16.3.
Kaspersky Endpoint Security en mode EDR Agent	Kaspersky Security Center Windows 14.2, 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2, 16.3.

Version prise en charge de Kaspersky Security for Virtualization Light Agent

L'application Kaspersky Endpoint Security peut être utilisé comme Light Agent dans le cadre de Kaspersky Security for Virtualization Light Agent version 6.5.

Versions des solutions prises en charge sur les plate-formes KATA et OSMP

Kaspersky Endpoint Security est compatible avec les solutions basées sur Kaspersky Anti Targeted Attack Platform et avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises) des versions suivantes :

- Kaspersky Anti Targeted Attack Platform 6.0, 6.1, 7.0, 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), y compris les scénarios d'envoi de fichiers à la Sandbox pour analyse).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA), y compris les scénarios d'envoi de fichiers à la Sandbox pour analyse).

  Pour plus d'informations sur la solution Kaspersky Anti Targeted Attack Platform, consultez l'aide de Kaspersky Anti Targeted Attack Platform.
- Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0, 8.1, 8.2 sur Open Single Management Platform (ci-après également dénommée OSMP), y compris les scénarios d'envoi de fichiers à la sandbox pour analyse.

  Pour plus d'informations sur Kaspersky Endpoint Detection and Response Expert (on-premises), consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on premises).

Versions de l'Agent d'administration prises en charge pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Pour intégrer l'application à Kaspersky Endpoint Detection and Response Expert (cloud), vous avez besoin d'un Agent d'administration pour Kaspersky Security Center Cloud Console dans les versions spécifiques décrites dans l'Aide de Kaspersky Security Center Cloud Console.

Compatibilité avec les solutions tierces

Kaspersky Endpoint Security en mode EDR Agent peut fonctionner conjointement avec l'application antivirus Dr. Web.

Comparaison des fonctionnalités des solutions Kaspersky

Kaspersky Endpoint Security est inclus dans de nombreuses solutions multiplateformes de Kaspersky. Les fonctionnalités disponibles de l'application sont déterminées par la solution que vous avez achetée auprès d'un prestataire de services de votre région.

Fonction	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert	Kaspersky Hybrid Cloud Security, Desktop	Kaspersky Hybrid Cloud Security Enterprise Desktop/CPU/Server	K C
Protection contre les fichiers malicieux	✓	✓	✓	✓	✓	✓	✓	✓	
Protection contre les menaces par emails	✓	✓	✓	✓	✓	✓	✓	✓	
Protection contre les menaces Internet	✓	✓	✓	✓	✓	✓	✓	✓	
Protection contre les menaces réseau	✓	✓	✓	✓	✓	✓	✓	✓	
Gestion du pare-feu	✓	✓	✓	✓	✓	✓	✓	✓	
Détection comportementale	✓	✓	✓	✓	✓	✓	✓	✓	
Protection BadUSB	–	✓	✓	✓	✓	✓	✓	✓	
Contrôle des appareils	✓	✓	✓	✓	✓	✓	✓	✓	
Analyse des disques amovibles.	✓	✓	✓	✓	✓	✓	✓	✓	
Protection contre le chiffrement (pour les dossiers partagés)	✓	✓	✓	–	✓	✓	–	✓	
Analyser les conteneurs.	–	–	–	–	–	✓	–	✓	
Contrôle des applications	✓	✓	✓	✓	✓	✓	✓	✓	
Contrôle Internet	✓	✓	✓	✓	✓	✓	✓	✓	
Intégration avec Kaspersky Unified Monitoring and Analysis Platform	–	–	–	–	–	✓	–	–	
Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)	–	–	–	–	✓	✓	–	–	
Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)	–	–	–	–	✓	✓	–	–	

Kaspersky Endpoint Detection and Response Optimum	✓	✓	✓	✓	–	–	–	–
Intégration avec la solution Kaspersky Managed Detection and Response	–	–	–	✓	–	–	–	–

Déploiement et configuration initiale

Vous pouvez suivre ce scénario pour déployer l'application Kaspersky Endpoint Security et la préparer à l'utilisation.

1 Sélectionnez le mode d'utilisation de l'application

Après avoir acheté une solution Kaspersky sur le site Internet officiel de Kaspersky ou auprès de l'un de nos partenaires, vous recevrez un message à l'adresse email que vous avez indiquée lors de l'achat. Ce message contiendra un code d'activation et des informations sur la manière d'obtenir un fichier clé. Vous pouvez avoir besoin d'un fichier clé si votre organisation ne prend pas en charge l'activation en ligne de l'application à l'aide d'un code.

Votre choix de solution détermine les modes dans lesquels vous pouvez utiliser l'application :

- Si vous disposez d'une licence Kaspersky Endpoint Security, vous pouvez utiliser l'application en mode standard.
- Si vous disposez d'une licence Kaspersky Security for Virtualization Light Agent, vous pouvez utiliser l'application en mode Light Agent.
- Si vous disposez d'une licence Kaspersky Endpoint Detection and Response Expert (on-premises), vous pouvez utiliser l'application en mode agent EDR.

Le déploiement de l'application dépend du mode sélectionné.

Une fois Kaspersky Endpoint Security installé, il n'est pas possible de modifier le mode d'utilisation de l'application.

2 Préparation de l'environnement

Effectuez les actions préparatoires nécessaires en fonction de votre infrastructure.

3 Sélection du mécanisme d'interception des événements système

Si le système d'exploitation de votre appareil prend en charge fanotify, vous pouvez sélectionner lors de l'installation le mécanisme à utiliser pour intercepter les événements système.

4 Préparation des paquets de distribution

Téléchargez les fichiers nécessaires à l'installation de l'application. Les fichiers dont vous avez besoin dépendent du système d'exploitation de l'appareil protégé et de la méthode de déploiement de l'application.

5 Actions préparatoires dans Kaspersky Security Center

Effectuez les actions préparatoires dans Kaspersky Security Center. Nous vous recommandons d'utiliser Kaspersky Security Center pour l'administration centralisée de la protection de votre organisation. Kaspersky Security Center est également requis si vous utilisez Kaspersky Endpoint Security en mode agent EDR ou en mode Light Agent.

6 Installation de l'application

Installez l'application sur les appareils selon la méthode qui convient aux besoins de votre organisation :

- Installation de l'application à l'aide de Kaspersky Security Center
- Installation de l'application à l'aide d'une ligne de commande

7 Étapes de configuration supplémentaires après l'installation sous certains systèmes d'exploitation

Certains systèmes d'exploitation Linux nécessitent une configuration supplémentaire après l'installation de Kaspersky Endpoint Security.

Modes et schémas de déploiement

Kaspersky Endpoint Security fait partie de nombreuses solutions Kaspersky. Le choix de la solution détermine le mode de fonctionnement et le schéma de déploiement de l'application.

Mode standard

Mode par défaut de l'application. Kaspersky Endpoint Security offre une protection complète aux postes de travail et aux serveurs Linux contre différents types de menaces, d'attaques réseau et de fraude.

Dans ce mode, l'application utilise des modules de protection et de contrôle des appareils, tels que Protection contre les fichiers malicieux ou Détection comportementale, ainsi que des agents intégrés pour assurer une protection contre les menaces avancées et les attaques ciblées.

Vous pouvez installer l'application dans ce mode dans le cadre des solutions Kaspersky EPP (Endpoint Protection Platform). Par exemple, Kaspersky Endpoint Security en mode Standard fait partie de Kaspersky Endpoint Security for Business.

Le schéma de déploiement principal de Kaspersky Endpoint Security est le déploiement centralisé via Kaspersky Security Center. Sur chaque appareil protégé, vous devez installer Kaspersky Endpoint Security et le module Agent d'administration de Kaspersky Security Center. Ce module connecte les appareils au Serveur d'administration de Kaspersky Security Center et permet de les administrer à l'aide de Kaspersky Security Center.

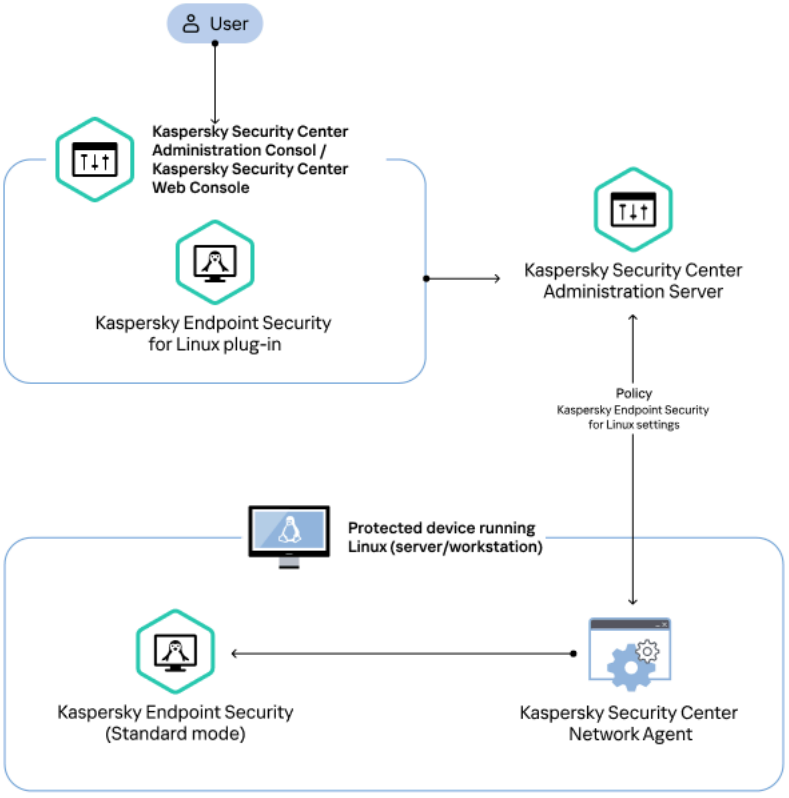


Schéma de déploiement de Kaspersky Endpoint Security en mode standard

Mode Endpoint Detection and Response Agent (EDR Agent)

Ce mode permet de déployer les solutions Kaspersky Detection and Response avec des solutions antivirus tierces. Les solutions Detection and Response incluent :

- Kaspersky Endpoint Detection and Response Expert (on-premises) sur Open Single Management Platform (ci-après également dénommé « OSMP »).
- Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sur Kaspersky Anti Targeted Attack Platform (ci-après également dénommée « KATA »).

En mode EDR Agent, les modules de protection et de contrôle tels que la Protection contre les fichiers malicieux ou la Protection contre les menaces Internet ne sont pas disponibles. Une application antivirus tierce protège l'appareil. L'agent EDR surveille en permanence les processus exécutés sur ces appareils, les connexions réseau ouvertes et les fichiers modifiés, et interagit avec les solutions Detection and Response pour assurer la protection contre les menaces avancées et les attaques ciblées.

Pour que Kaspersky Endpoint Security fonctionne en mode EDR Agent, vous devez déployer l'infrastructure appropriée ; pour en savoir plus, consultez la section de l'aide relative à la solution Detection and Response que vous avez sélectionnée. Pour en savoir plus sur les particularités du mode EDR Agent, consultez l'article Problèmes connus et limitations.

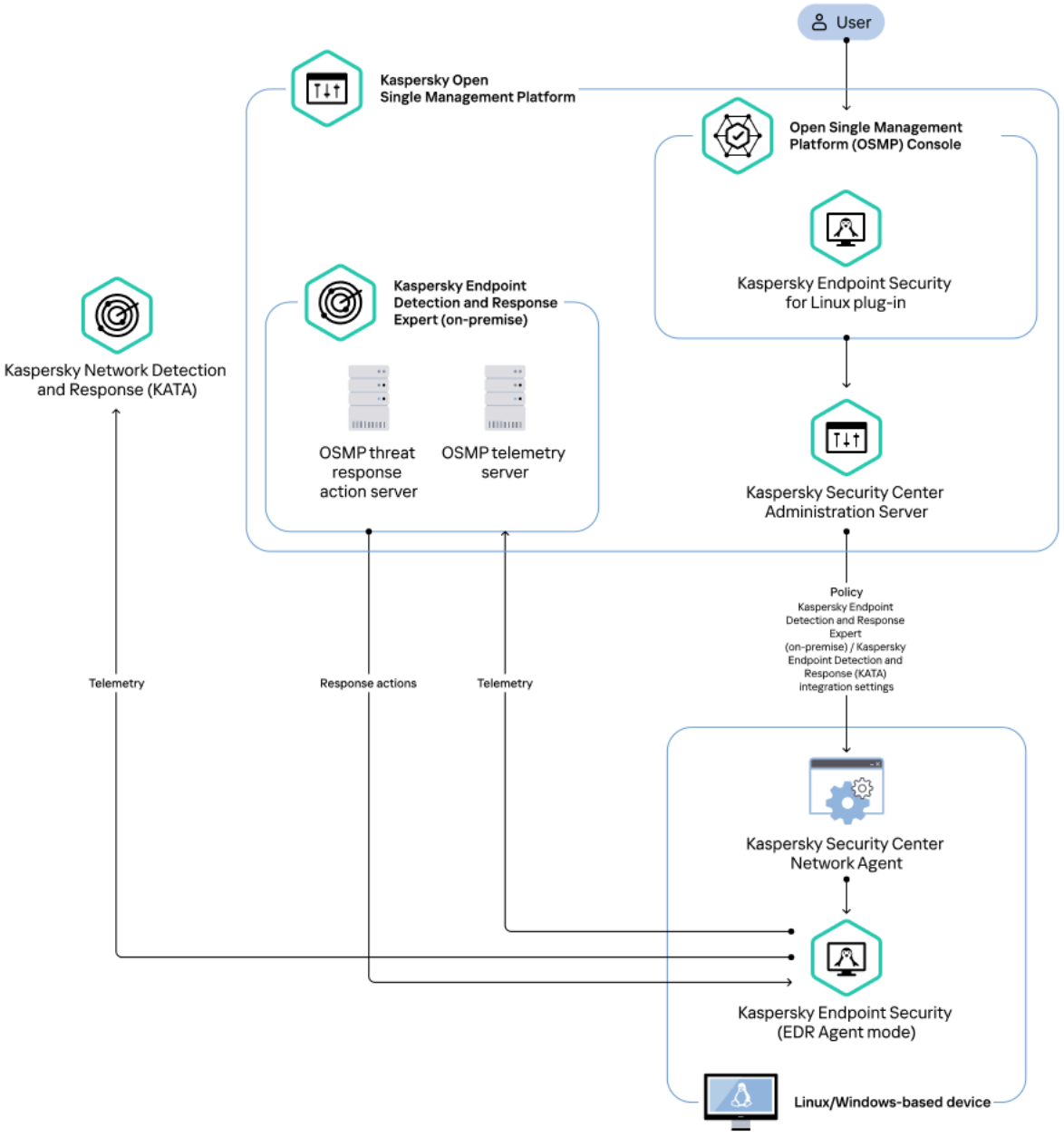


Schéma de déploiement de Kaspersky Endpoint Security en mode EDR Agent avec Kaspersky Endpoint Detection and Response Expert (on-premises)

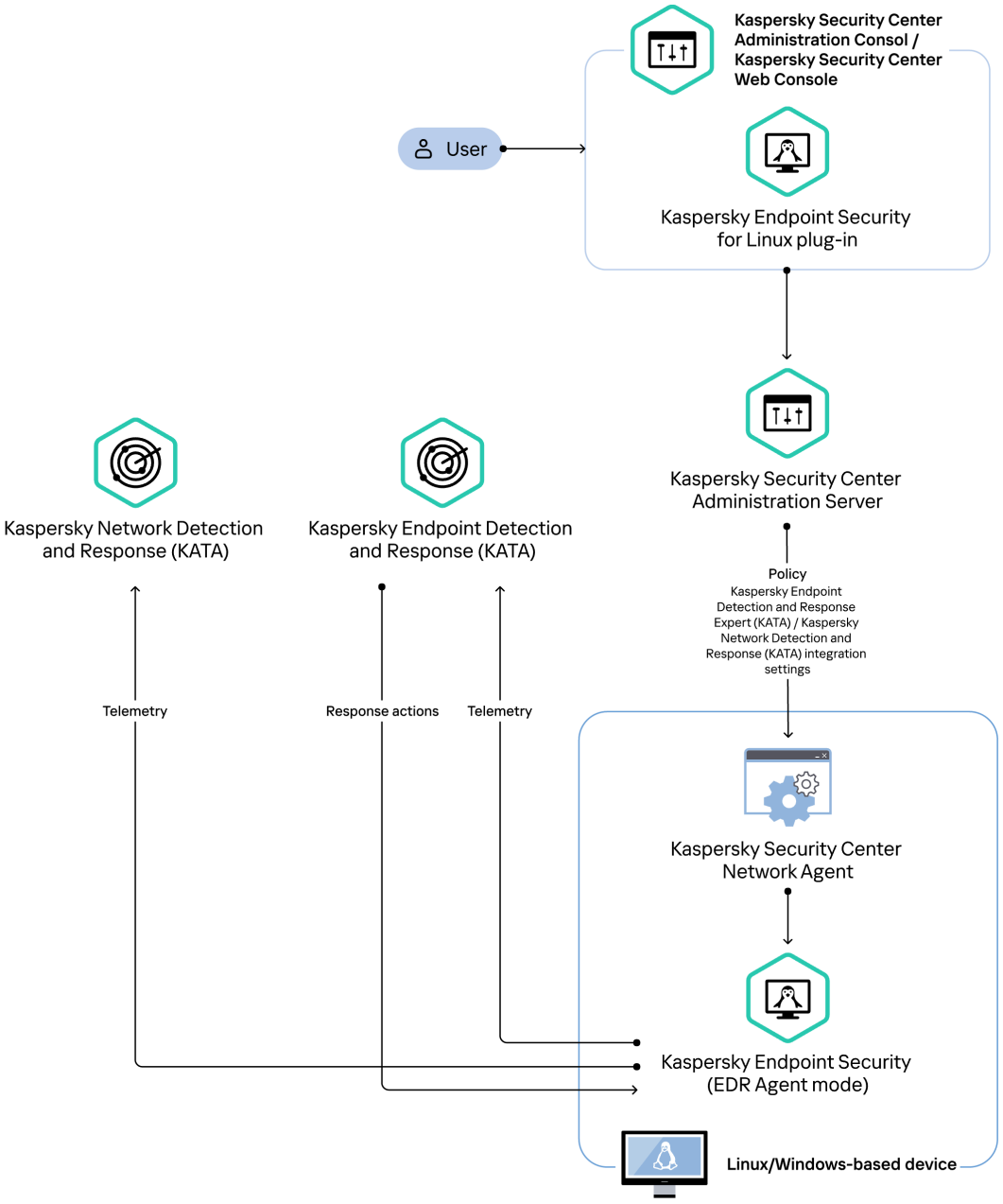


Schéma de déploiement de Kaspersky Endpoint Security en mode EDR Agent avec Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response

Mode Light Agent

Kaspersky Endpoint Security en mode Light Agent fait partie de la solution Kaspersky Security for Virtualization Light Agent destinée à protéger les machines virtuelles exécutant des systèmes d'exploitation invités Linux.

Les mêmes modules de protection et de contrôle sont disponibles dans ce mode et dans le mode Standard. La différence est que les objets sont analysés à la recherche de virus et d'autres applications malveillantes, que les clés de licence sont ajoutées et que les bases de données et les modules sont mis à jour par un module spécial de la solution installé sur une machine virtuelle distincte, la SVM (Secure Virtual Machine). Cela permet de réduire la charge de l'hyperviseur, car l'application en mode Light Agent utilise les ressources de la SVM pour protéger l'infrastructure au lieu de celles des machines virtuelles.

Pour que Kaspersky Endpoint Security fonctionne en mode Light Agent, vous devez déployer l'infrastructure appropriée ; pour en savoir plus, consultez l'Aide de Kaspersky Security for Virtualization Light Agent. Pour en savoir plus sur les particularités du mode Light Agent, consultez l'article Problèmes connus et limitations.

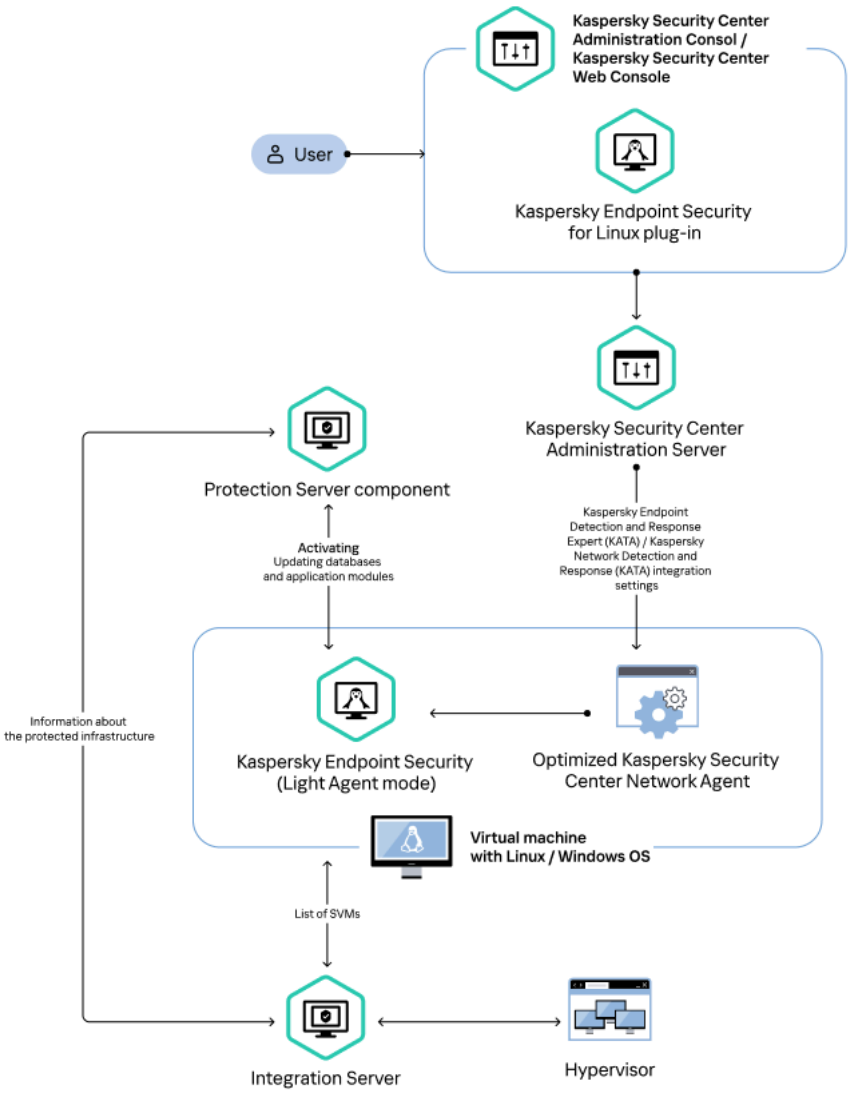


Schéma de déploiement de Kaspersky Endpoint Security en mode Light Agent

Après avoir sélectionné le mode de l'application, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Préparation de l'environnement.

Préparation de l'environnement pour l'installation de l'application

Préparation de l'infrastructure

Kaspersky Security Center

Si vous envisagez une administration centralisée de l'application à l'aide de Kaspersky Security Center, installez Kaspersky Security Center dans votre infrastructure. Si vous avez déjà installé Kaspersky Security Center Windows et prévoyez de migrer vers Kaspersky Security Center Linux, suivez ces instructions : Migration des données vers Kaspersky Security Center Linux.

Kaspersky Endpoint Security en mode Agent EDR

Pour que Kaspersky Endpoint Security fonctionne en mode EDR Agent, vous devez déployer l'infrastructure appropriée ; pour en savoir plus, consultez la section de l'aide relative à la solution Detection and Response que vous avez sélectionnée.

Kaspersky Endpoint Security en mode Light Agent

Pour que Kaspersky Endpoint Security fonctionne en mode Light Agent, vous devez déployer la solution Kaspersky Security for Virtualization Light Agent :

1. Installez les modules de la solution Kaspersky Security for Virtualization Light Agent, à savoir le Serveur d'intégration et le Serveur de protection.
2. Préparez le Serveur de protection au fonctionnement en activant la solution et en configurant les mises à jour des bases de données pour le Serveur de protection et les Light Agents.

   Pour plus d'informations sur l'installation et la configuration des modules de la solution, consultez l'aide de Kaspersky Security for Virtualization Light Agent.
3. Assurez-vous que les machines virtuelles que vous souhaitez protéger répondent aux exigences du mode Light Agent.
4. Assurez-vous que les paramètres de l'équipement réseau ou du logiciel qui contrôle le trafic entre les machines virtuelles permettent au trafic réseau de passer par les ports utilisés pour l'interaction entre l'application Kaspersky Endpoint Security en mode Light Agent et les autres modules de Kaspersky Security for Virtualization Light Agent. Les ports utilisés par le Light Agent sont répertoriés dans l'aide de Kaspersky Security for Virtualization Light Agent.

Le mode Light Agent de Kaspersky Endpoint Security n'est pas pris en charge sur les appareils basés sur l'architecture Arm ni sur ceux équipés d'un processeur Elbrus.

Préparation de l'appareil pour l'installation

- Vérifiez que votre appareil répond aux exigences matérielles et logicielles de l'application.
- Si vous souhaitez installer Kaspersky Endpoint Security en mode standard ou en mode Light Agent, assurez-vous qu'aucun logiciel antivirus tiers n'est installé sur votre appareil. En mode Agent EDR, Kaspersky Endpoint Security peut fonctionner avec l'application Dr. Web.
- Assurez-vous que l'application Kaspersky Endpoint Agent for Linux n'est pas installée sur votre appareil. Si Kaspersky Endpoint Agent for Linux est installé, désinstallez-le.
- Assurez-vous que l'utilitaire iptables est installé sur votre appareil. L'application requiert l'utilitaire iptables pour intercepter le trafic réseau.

- Assurez-vous que root est le propriétaire des répertoires suivants et que seul le propriétaire dispose d'un accès en écriture : /var, /var/opt, /opt, /usr/bin, /usr/lib, /usr/lib64. Cette opération est nécessaire pour que l'application démarre et fonctionne correctement.

- Lorsque l'application est en cours d'exécution, le système d'exploitation peut utiliser beaucoup plus de descripteurs de fichier. Assurez-vous que la limite du nombre de descripteurs est suffisamment élevée. Pour vérifier la limite, exécutez la commande `cat /proc/sys/fs/file-max`. En règle générale, nous recommandons de désactiver la limite en spécifiant `fs.file-max=9223372036854775807` dans le fichier /etc/sysctl.conf. Après avoir effectué cette modification, redémarrez le système d'exploitation.

- Assurez-vous que `kernel.yama.ptrace_scope=0` dans le système d'exploitation. D'autres valeurs du paramètre `kernel.yama.ptrace_scope` peuvent affecter le fonctionnement de l'application Kaspersky Endpoint Security ; pour plus de détails, consultez la section Problèmes connus et limitations.

En outre, pour installer l'interface graphique de l'application :

- La version du paquet kesl-gui que vous installez doit correspondre à la version de votre paquet kesl.

- Pour que l'interface graphique de Kaspersky Endpoint Security fonctionne correctement, l'utilitaire Zenity doit être installé dans votre système d'exploitation.

- Si votre appareil a accès aux dépôts du gestionnaire de paquets, toutes les dépendances nécessaires sont installées automatiquement lors de l'installation de l'interface graphique de l'application. Si l'appareil se trouve dans un segment privé et n'a pas accès aux dépôts du gestionnaire de paquets :

  1. Vérifiez la liste des dépendances sur un appareil de référence (libice6, libsm6, zlib1g, kesl).

  2. Exécutez une des actions suivantes :

     - Avant d'installer l'interface graphique, téléchargez les paquets sur tous les appareils, puis installez-les à l'aide du gestionnaire de paquets.

     - Assurez-vous que les paquets sont téléchargés sur les appareils lors de l'installation de l'interface graphique.

En outre, pour la prise en charge du plug-in MMC

Si vous prévoyez d'utiliser la Console d'administration de Kaspersky Security Center pour administrer l'application, installez Microsoft® Visual C++® 2015 Redistributable Update 3 RC sur l'appareil sur lequel le Serveur d'administration est installé (voir https://www.microsoft.com/fr-fr/download/details.aspx?id=52685). Cette opération est nécessaire au fonctionnement du plug-in d'administration MMC de Kaspersky Endpoint Security.

En outre, pour certains systèmes d'exploitation

Astra Linux en mode d'environnement logiciel fermé

Installation du pack de compatibilité

Vous devez installer le pack de compatibilité dans les cas suivants :

- Avant d'installer l'application en mode d'environnement logiciel fermé.
- Si l'application est déjà installée, lors du passage du système d'exploitation en mode d'environnement logiciel fermé.

Paquet d'installation

```
apt install astra-digsig-oldkeys
```

Cela permettra d'exécuter l'application sur les systèmes d'exploitation Astra Linux Special Edition (mises à jour 4.7 pour l'architecture Arm, 1.6, 1.7 et 1.8) en mode d'environnement logiciel fermé.

Réautorisation de ptrace

Dans les systèmes d'exploitation Astra Linux, la fonction d'interdiction du traçage ptrace (Disable ptrace capability) est activée par défaut, ce qui peut affecter le fonctionnement de l'application Kaspersky Endpoint Security. Pour un fonctionnement correct de Kaspersky Endpoint Security, il est recommandé de désactiver l'interdiction de traçage ptrace lors de l'installation d'Astra Linux. Si Astra Linux est déjà installé, consultez le site Web du centre d'aide Astra Linux pour obtenir des instructions sur l'activation et la désactivation de ce mode (**Configuration des mécanismes de protection et de blocage**, section **Blocage des traçages ptrace**).

SUSE Linux Enterprise Server 15

Avant d'installer l'application sur un appareil sous SUSE Linux Enterprise Server 15, installez le paquet insserv-compat.

ALT SP en mode d'environnement logiciel fermé

Avant d'installer l'application sur un appareil doté du système d'exploitation ALT SP en mode d'environnement logiciel fermé :

1. Désactivez le mode d'environnement logiciel fermé :

   ```
   integrity-remover
   ```

2. Créez un groupe kesl en vue des modifications ultérieures de la stratégie IMA :

   ```
   groupadd kesl
   ```

3. Déterminez l'identifiant unique (GID) du groupe créé :

   ```
   cat /etc/group | grep kesl
   ```

4. Modifiez la stratégie IMA pour exclure le groupe kesl de la vérification de l'intégrité des modules de l'application à l'aide de l'utilitaire, afin de vous assurer que l'application fonctionne correctement. Pour ce faire, procédez comme suit :

   a. Copiez le fichier /usr/share/integrity/policy :

   ```
   cp /usr/share/integrity/policy /etc/integrity/policy
   ```

b. Ouvrez le fichier /etc/integrity/policy pour le modifier dans un éditeur de texte (par exemple, vim) :

```
vim /etc/integrity/policy
```

c. Après la ligne `dont_measure fsmagic=0xf97cff8c` (il s'agit généralement de la dernière ligne de la section `dont_measure`), ajoutez la ligne :

```
dont_measure fgroup=<GID>
```

où `<GID>` est un identifiant unique du groupe créé à l'étape 2 de ces instructions.

d. Après la ligne `dont_appraise fsmagic=0x27e0eb` (il s'agit généralement de la dernière ligne de la section `dont_appraise`), ajoutez la ligne :

```
dont_appraise fgroup=<GID>
```

où `<GID>` est un identifiant unique du groupe créé à l'étape 2 de ces instructions.

e. Enregistrez vos modifications.

5. Dans le fichier /usr/sbin/integrity-sign, modifiez la fonction list_all_files pour inclure Kaspersky Endpoint Security dans la liste d'autorisation des applications autorisées à s'exécuter en mode environnement logiciel fermé. Pour ce faire, procédez comme suit :

a. Ouvrez le fichier /usr/sbin/integrity-sign pour le modifier dans un éditeur de texte (par exemple, vim) :

```
vim /usr/sbin/integrity-sign
```

b. Recherchez la fonction list_all_files et dans le corps de la fonction, dans les lignes commençant par `find -P` à la fin de chaque liste de répertoire, ajoutez les répertoires de l'application Kaspersky Endpoint Security /var/opt et /opt.

c. Enregistrez vos modifications.

Lors de la configuration initiale de l'application, ne lancez pas la mise à jour des bases de données de l'application.

Une fois l'installation de l'application terminée, effectuez les étapes nécessaires au démarrage.

OSnova

Si vous prévoyez d'utiliser Kaspersky Security Center pour installer et gérer l'application, préparez l'appareil en vue de l'installation de l'Agent d'administration avant d'installer l'application :

1. Ouvrez le fichier /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf pour le modifier et, dans la section `[Login]`, commentez la ligne KillUserProcesses=yes.

```
#KillUserProcesses=yes
```

2. Ouvrez le fichier /usr/lib/NESS/pam-user-session pour le modifier et commentez la ligne loginctl terminate-session "$XDG_SESSION_ID".

```
#loginctl terminate-session "$XDG_SESSION_ID"
```

Systèmes d'exploitation prenant en charge SELinux

Si l'utilitaire semanage n'est pas installé dans votre système d'exploitation, avant d'installer l'application, installez le paquet policycoreutils-python ou policycoreutils-python-utils, selon votre gestionnaire de paquets.

Le paquet policycoreutils-python-utils est fourni pour les types de gestionnaires de paquets suivants : dnf, apt et yum pour Fedora, Debian, Ubuntu et RHEL 7 et versions ultérieures.

Le paquet policycoreutils-python est fourni pour les types de gestionnaires de paquets suivants : yum pour CentOS/RHEL 7 et versions antérieures.

Kylin OS

Avant d'installer l'application sur un appareil Kylin OS :

1. Dans l'UKUI (Ubuntu Kylin User Interface), désactivez le Firewall. Pour ce faire, accédez à la section **Centre de sécurité Kylin** → **Pare-feu et protection du réseau** et, sous le **Pare-feu**, désactivez les commutateurs **Réseau public** et **Réseau privé**.

2. Dans l'UKUI, désactivez le Contrôle réseau des applications. Pour ce faire, accédez à la section **Centre de sécurité Kylin** → **Pare-feu et protection du réseau** et, sous **Contrôle réseau des applications**, sélectionnez **Désactiver**.

3. Dans l'UKUI, désactivez la Vérification de la source de l'application. Pour ce faire, accédez à la section **Centre de sécurité Kylin** → **Protection des applications** et, sous **Vérification de la source de l'application**, sélectionnez **Désactiver**.

4. Désactivez le mécanisme de sécurité KYSEC. Pour ce faire, effectuez les actions suivantes dans le terminal :

   a. Vérifiez l'état actuel :

   ```
   getstatus
   ```

   b. Désactivez le mécanisme de sécurité KYSEC :

   ```
   setstatus disable -p
   ```

   c. Vérifiez que le mécanisme de sécurité KYSEC est désactivé :

   ```
   getstatus
   ```

5. Désinstallez l'application antivirus intégrée. Pour ce faire, exécutez la commande suivante dans le terminal :

```
sudo dpkg -P pksav
```

6. Si l'antivirus Qaxsafe est installé sur votre appareil, vous devez le désinstaller. Pour ce faire, procédez comme suit :

   a. Désactivez l'autoprotection :

      1. Recherchez l'icône de l'application dans la zone de notification de la barre des tâches et double-cliquez sur l'icône de l'application pour ouvrir le menu contextuel.

      2. Dans le menu contextuel, sélectionnez **Paramètres** → **Centre de protection**.

      3. Une fenêtre s'ouvre ; dans cette fenêtre, décochez la case **Activer l'autoprotection** et saisissez un mot de passe si vous y êtes invité.

   b. Désinstallez l'antivirus Qaxsafe. Pour ce faire, exécutez la commande suivante dans le terminal :

   ```
   sudo dpkg -P qaxsafe
   ```

   c. Supprimez les fichiers restants. Pour ce faire, exécutez la commande suivante dans le terminal :

   ```
   sudo rm -rf /opt/qaxsafe
   ```

Systèmes d'exploitation qui ne prennent pas en charge fanotify

Avant de procéder à l'installation de l'application, assurez-vous que les éléments suivants sont installés sur l'appareil :

- paquets pour compiler des applications et exécuter des tâches (gcc, binutils, glibc, glibc-devel, make) ;
- Paquet contenant les fichiers d'en-tête du noyau du système d'exploitation pour la compilation des modules de Kaspersky Endpoint Security

Articles utiles

Résolution des problèmes sur Kylin OS

Après avoir préparé l'environnement pour l'installation, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Sélection du mécanisme d'interception des événements système.

Sélection du mécanisme d'interception des événements système

Pour fonctionner correctement, l'application doit intercepter les événements système relatifs aux opérations sur les fichiers et au lancement des processus. L'interception des événements système est requise dans tous les modes de l'application (mode standard, mode Light Agent et mode agent EDR). Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Mécanisme d'interception des événements système

L'application peut utiliser les mécanismes suivants pour intercepter les événements système :

- **Mécanisme d'interception du système basé sur la technologie fanotify.** *Fanotify* est un sous-système du noyau Linux qui surveille les événements dans le système de fichiers (par exemple, l'ouverture, la lecture, l'écriture ou la fermeture de fichiers) et permet aux applications de les intercepter en temps réel.

- **Mécanisme d'interception basé sur un module de noyau mis à jour.** Le *module de noyau mis à jour* fonctionne conjointement avec le mécanisme d'interception système basé sur la technologie fanotify. Cela permet d'optimiser l'interception des opérations sur les fichiers et l'interception des lancements de processus par Kaspersky Endpoint Security en traitant les événements système dans kernel space, et non dans user space. Le module de noyau mis à jour intercepte les opérations sur les fichiers lors de l'ouverture, du renommage et de la modification des fichiers. Les performances de l'application sont améliorées grâce au cache des résultats de l'analyse des fichiers et des processus.

  Le module de noyau mis à jour est également utilisé pour les tâches et les modules suivants :

  - Protection contre les fichiers malicieux
  - Protection contre le chiffrement
  - Protection contre les exploits
  - Détection comportementale
  - Contrôle des applications
  - Prévention de l'exécution pour les objets (lors de l'intégration à Kaspersky Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response Optimum)

  Lors de l'utilisation d'un module de noyau mis à jour, vous pouvez configurer plus précisément les exclusions globales. Le mécanisme d'interception basé sur la technologie fanotify permet d'exclure totalement l'interception des opérations sur les fichiers pour les points de montage indiqués. Le module de noyau mis à jour vous permet d'exclure des répertoires locaux ou distants spécifiques montés sur l'appareil.

  Le module de noyau mis à jour est inclus avec l'application.

- **Module de noyau pour la Protection contre les fichiers malicieux sur un système d'exploitation sans fanotify**. Si le système d'exploitation de l'appareil ne prend pas en charge la technologie fanotify (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), l'application compile et utilise un module spécial pour intercepter les événements système. Ce module est automatiquement compilé au lancement de la Protection contre les fichiers malicieux, à condition que les paquets de compilation et les utilitaires nécessaires soient disponibles.

Comment choisir un mécanisme d'interception des événements système

Si le système d'exploitation prend en charge fanotify, vous pouvez sélectionner un mécanisme d'interception des événements système lors du déploiement de l'application : fanotify uniquement ou module de noyau mis à jour avec fanotify. Le paramètre par défaut est fanotify. Après l'installation, vous pouvez modifier le mécanisme d'interception des événements système dans les paramètres de l'application.

Pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, le choix du mécanisme d'interception n'est pas disponible.

Une application peut utiliser le mécanisme d'interception basé sur le module de noyau mis à jour si le système d'exploitation répond aux exigences d'installation du module de noyau mis à jour.

Configuration requise pour l'installation du module de noyau mis à jour

Pour installer et utiliser le module de noyau mis à jour, l'appareil doit disposer de l'un des systèmes d'exploitation 64 bits suivants :

- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6.5, 1.6.6).
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7.3, 1.7.4, 1.7.6, 1.7.7, 1.7.8, 1.7.9).
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8.2, 1.8.3, 1.8.4, 1.8.5).

  Si Kaspersky Endpoint Security est utilisé en mode standard, le module de noyau mis à jour peut être utilisé sur les appareils exécutant des systèmes d'exploitation Astra Linux en mode environnement logiciel fermé.

- CentOS 7.x.
- CentOS 8.x.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.0.1
- SberLinux 9.1.
- SberLinux 9.6.
- SberLinux 9.7.
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS.

- ALT SP Workstation version 10.
- ALT SP Server version 10.
- ALT Education 10.
- ALT Workstation 11.
- ALT Server 11
- ALT Education 11.
- RED OS 7.3
- RED OS 8.0
- ROSA « Cobalt » 7.9 Workstation.
- ROSA « Cobalt » 7.9 Server.
- ROSA « Chrome » 12 Workstation.
- ROSA « Chrome » 12 Server.

Les systèmes d'exploitation 32 bits, les systèmes d'exploitation pour l'architecture Arm et les systèmes d'exploitation pour l'architecture Elbrus ne sont pas pris en charge.

Il peut y avoir des conflits dans le fonctionnement du module de noyau mis à jour sur les appareils dotés de certaines versions de noyaux du système d'exploitation Linux, ainsi que lors de l'utilisation de certaines applications tierces.

Vérification de la possibilité d'installer un module du noyau à actualiser

La version du module de noyau mis à jour ne dépend pas de la version de Kaspersky Endpoint Security. Les fonctionnalités du module de noyau mis à jour sont régulièrement étendues dans le cadre des mises à jour des bases de données et des modules de l'application de Kaspersky Endpoint Security. Par conséquent, la liste des systèmes d'exploitation pris en charge ci-dessus peut ne pas être exhaustive. Pour vérifier que votre appareil répond aux exigences d'installation du module de noyau mis à jour, utilisez l'outil Kaspersky ULKM.

Procédure de vérification à distance à l'aide de la Web Console ou de la Console d'administration

1. Téléchargez l'archive ulkmtool.zip depuis la page de téléchargement de l'application dans la section **Kaspersky Endpoint Security for Linux**.
2. Créez un paquet d'installation pour l'utilitaire.

Comment créer un paquet d'installation dans Web Console

1. Placez l'archive téléchargée ulkmtool.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center.

2. Dans la fenêtre principale de Web Console, sélectionnez l'une des sections suivantes :

   - **Découverte et déploiement des appareils → Déploiement et attribution → Paquets d'installation**.
   - **Opérations → Stockages → Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

3. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création du paquet d'installation démarre.

4. Sélectionnez le mode de création du paquet d'installation : **Créer un paquet d'installation à partir d'un fichier**.

5. Saisissez le nom du nouveau paquet d'installation, cliquez sur le bouton **Parcourir** et spécifiez le chemin d'accès à l'archive ulkmtool.zip que vous avez téléchargée.

6. Quittez l'Assistant.

Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

Comment créer un paquet d'installation dans la Console d'administration

1. Décompressez l'archive ulkmtool.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Avancés → Installation à distance → Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

3. Cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du paquet d'installation démarre.

4. Cliquez sur le bouton **Créer un paquet d'installation pour l'application Kaspersky**.

5. Saisissez le nom du nouveau paquet d'installation, puis passez à l'étape suivante de l'Assistant.

6. Cliquez sur le bouton **Parcourir** et spécifiez le chemin d'accès au fichier ulkmtool.kud. Le fichier se trouve dans le dossier où vous avez décompressé l'archive ulkmtool.zip.

   Passez à l'étape suivante de l'Assistant.

7. Attendez que le fichier soit téléchargé et quittez l'Assistant.

Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

3. Installez l'Agent d'administration de Kaspersky Security Center sur les appareils dont vous souhaitez vérifier la conformité avec les exigences d'installation du module de noyau mis à jour. Consultez l'aide de Kaspersky Security Center pour plus de détails.

4. Dans Kaspersky Security Center Web Console ou la Console d'administration, créez et exécutez une tâche d'Installation à distance sur les appareils pour lesquels vous souhaitez vérifier qu'ils répondent aux exigences du module de noyau mis à jour. Dans les paramètres de la tâche, sélectionnez le paquet d'installation que vous avez créé.

   Les résultats de l'exécution de la tâche pour chaque appareil sur lequel la tâche a été exécutée indiquent si l'appareil prend en charge l'installation et le fonctionnement du module de noyau mis à jour.

En fonction des résultats de la tâche, une étiquette est automatiquement attribuée à chaque appareil :

- *UpdatableKernelModule=No* : l'appareil ne prend pas en charge l'installation d'un module de noyau mis à jour.
- *UpdatableKernelModule=Oui* : l'appareil répond aux exigences d'installation et d'exécution d'un module de noyau mis à jour.

Vous pouvez utiliser ces tags pour créer des sélections d'appareils. Par exemple, vous pouvez sélectionner des appareils qui répondent aux exigences du module de noyau mis à jour et installer l'application Kaspersky Endpoint Security avec le module de noyau mis à jour sur ces appareils.

Procédure de vérification locale sur l'appareil

1. Téléchargez l'archive ulkmtool.zip depuis la page de téléchargement de l'application dans la section **Kaspersky Endpoint Security for Linux**.
2. Installez l'Agent d'administration de Kaspersky Security Center sur les appareils dont vous souhaitez vérifier la conformité avec les exigences d'installation du module de noyau mis à jour. Consultez l'aide de Kaspersky Security Center pour plus de détails.
3. Exécutez l'utilitaire Kaspersky ULKM tool localement sur les appareils que vous souhaitez analyser.

   ```
   ulkmtool --check remote
   ```

4. Vérifiez le code de retour.

   ```
   echo $?
   ```

   L'utilitaire renvoie les codes suivants sur la ligne de commande :

   0 = Réussite signifie que l'appareil répond aux exigences d'installation et d'exécution du module de noyau mis à jour.

   1 = Non pris en charge signifie que l'appareil ne prend pas en charge l'installation du module de noyau mis à jour.

Vérification de l'état du module de noyau mis à jour

Dans Kaspersky Security Center Web Console ou la Console d'administration, vous pouvez vérifier l'état du module de noyau mis à jour sur les appareils dotés de Kaspersky Endpoint Security. Pour ce faire, vous pouvez afficher les tags attribués aux appareils :

- *UpdatableKernelModule=Use* : l'appareil dispose d'un module de noyau mis à jour installé et en cours d'exécution.
- *UpdatableKernelModule=Error* : un module de noyau pouvant être mis à jour est installé sur l'appareil, mais une erreur s'est produite lors du démarrage du module, le module ne fonctionne pas.

Pour obtenir plus de détails sur l'affichage des tags attribués aux appareils, consultez l'aide de Kaspersky Security Center.

Prise en charge du démarrage sécurisé

Le module de noyau mis à jour prend en charge Secure Boot. Pour utiliser le mécanisme d'interception basé sur le module de noyau mis à jour sur les systèmes d'exploitation sur lesquels Secure Boot est activé, vous devez ajouter au système d'exploitation le certificat public de Kaspersky Endpoint Security avec lequel le module est signé, puis redémarrer le système d'exploitation.

Télécharger le certificat

Exemple d'ajout d'un certificat pour Ubuntu

1. Assurez-vous que le démarrage sécurisé est activé dans votre système d'exploitation :

   ```
   mokutil --sb-state
   ```

2. Ajoutez le certificat téléchargé à votre système d'exploitation à l'aide de l'utilitaire mokutil :

   ```
   mokutil --import <path to certificate>
   ```

3. Redémarrez le système d'exploitation et confirmez l'importation du certificat dans le menu de MOK Manager.

4. Vérifiez que le module de noyau mis à jour fonctionne en exécutant la commande suivante :

   ```
   kesl-control --app-info
   ```

Après avoir sélectionné le mécanisme d'interception des événements système, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Préparation des paquets de distribution.

Préparation des paquets de distribution

Le *paquet de distribution de Kaspersky Endpoint Security* est un ensemble de fichiers pour l'installation et la mise à jour de l'application, ainsi que les textes des contrats d'utilisation (Contrat de licence utilisateur final, Politique de confidentialité et Déclaration de Kaspersky Security Network). Vous pouvez également télécharger séparément le paquet de distribution qui inclut une interface graphique afin de faciliter la gestion et la surveillance locales de l'application.

Vous aurez besoin des paquets de distribution pour créer un paquet d'installation en vue du déploiement sur les appareils du réseau d'entreprise à l'aide de Kaspersky Security Center, ainsi que pour déployer l'application à l'aide de la ligne de commande.

Pour le déploiement à l'aide de Kaspersky Security Center, vous aurez également besoin d'un *paquet de distribution pour l'installation à distance de l'application*. Ce paquet de distribution contient les fichiers nécessaires au déploiement à distance de l'application et les textes des contrats d'utilisation.

> Les textes des contrats d'utilisation sont disponibles sur le site Internet de Kaspersky (dans la section **CLUF**), ainsi que dans le répertoire `/opt/kaspersky/kesl/doc/` après l'installation de l'application.

Vous pouvez choisir les paquets de distribution pour déployer Kaspersky Endpoint Security vous-même ou à l'aide de Kaspersky Security Center à l'étape Création d'un paquet d'installation.

Comment choisir un paquet de distribution pour le déploiement de Kaspersky Endpoint Security

Le choix des paquets de distribution dépend des facteurs suivants :

- Version de Kaspersky Endpoint Security : certifiée ou non certifiée
- Méthode de déploiement : à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande
- Format du paquet en fonction du système d'exploitation
- Architecture du système d'exploitation et type de processeur
- Méthode d'administration de Kaspersky Endpoint Security
- Nécessité d'installer l'interface graphique de l'application

1. **Déterminez si votre version de l'application est certifiée ou non certifiée**

   - Si vous avez besoin de la version **certifiée**, téléchargez l'ensemble des paquets de distribution depuis la page Cycle de vie du support des applications pour entreprises.

     La version certifiée contient les fichiers principaux de l'application et les fichiers de l'interface graphique (le répertoire `kesl`), une archive pour l'installation à distance de l'application (le répertoire `remote install`), le plug-in MMC (`SCPlugin`) et le plug-in Internet (`web plugin`).

     Passez à l'étape 3.

   - Si vous avez besoin de la version **non certifiée**, passez à l'étape suivante.

2. **Déterminez la méthode de déploiement : à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande**

   Pour le **déploiement à l'aide de Kaspersky Security Center**, téléchargez le paquet de distribution depuis l'une des sources :

   - Depuis le site Internet de Kaspersky
   - En adressant une demande au Support technique si vous disposez d'un compte Kaspersky CompanyAccount

Pour le **déploiement à l'aide de la ligne de commande**, téléchargez le paquet de distribution depuis le site Internet de Kaspersky :

- Le paquet de distribution principal de l'application (`Distributive`)
- Le cas échéant, le paquet de distribution contenant l'interface graphique (`Product GUI`)

Si vous voulez télécharger les paquets de distribution depuis le site Internet de Kaspersky, vous aurez besoin des fichiers suivants :

- Le paquet de distribution principal de l'application (`Distributive`)
- Le cas échéant, le paquet de distribution contenant l'interface graphique (`Product GUI`)
- Paquet de distribution pour l'installation à distance de l'application à l'aide de Kaspersky Security Center (**Distributif complémentaire** → `Files for Product remote installation`)
- Paquet de distribution de l'Agent d'administration de Kaspersky Security Center (section des distributions de Kaspersky Security Center → `Network agent`)

Le paquet de distribution de l'application est le même pour toutes les localisations. La langue de Kaspersky Endpoint Security est sélectionnée lors de la configuration initiale de l'application. La prise en charge de la localisation dépend des langues installées dans le système d'exploitation.

3 Déterminez le format du paquet en fonction du système d'exploitation de l'appareil protégé

Système d'exploitation	Format du paquet
Debian, Ubuntu, Astra Linux, Linux Mint	`.deb`
Red Hat Enterprise Linux, CentOS, Oracle Linux, RED OS, SUSE Linux Enterprise, openSUSE, Rocky Linux, AlmaLinux, systèmes d'exploitation de la série ALT, GosLinux, systèmes d'exploitation de la série Rosa, Amazon Linux 2023	`.rpm`

Si votre système d'exploitation ne figure pas dans la liste, sélectionnez le format du paquet conformément à la documentation de votre système d'exploitation.

4 Déterminez l'architecture du système d'exploitation et le type de processeur

Type de processeur et nombre de bits du système d'exploitation	Paquet d'installation
Processeur Arm, système d'exploitation 64 bits	`arm64` `aarch64`
Processeur Elbrus	`e2k`
Autres processeurs, système d'exploitation 32 bits	`i386`

Autres processeurs, système d'exploitation 64 bits	`x86_64`
	`x64`
	`amd64`

Pour installer l'application Kaspersky Endpoint Security sur des systèmes d'exploitation à prise en charge limitée (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), sélectionnez le paquet de distribution portant la mention `OLD`.

Si vous décidez de modifier vous-même les fichiers de configuration de l'application d'une manière non décrite dans la documentation de l'application ou dans les recommandations des experts du Support technique, ces modifications pourraient entraîner des ralentissements et des pannes dans le fonctionnement de l'application et du système d'exploitation, une diminution du niveau de protection de votre appareil, une violation de la disponibilité et de l'intégrité des informations traitées ainsi que l'activation de l'envoi de statistiques complémentaires à KSN.

Après avoir préparé les paquets de distribution, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Actions préparatoires dans Kaspersky Security Center.

Actions préparatoires dans Kaspersky Security Center

Avant d'installer l'application Kaspersky Endpoint Security, nous vous recommandons d'effectuer les actions suivantes dans Kaspersky Security Center.

1 Configuration des groupes d'administration pour les appareils

Pour administrer l'application à l'aide de Kaspersky Security Center, vous devez placer les appareils sur lesquels l'application est installée dans des groupes d'administration. Par défaut, Kaspersky Security Center déplace tous les appareils sur lesquels l'Agent d'administration est installé et qui sont connectés au Serveur d'administration vers le groupe **Appareils non définis**.

Nous vous recommandons de configurer à l'avance les règles de placement automatique des appareils dans les groupes d'administration et de répartir les appareils dans des groupes en fonction de leur type, en créant un groupe distinct pour chaque type d'appareil. Cela vous permet d'appliquer différents paramètres de l'application selon l'appareil.

Vous pouvez également placer manuellement des appareils dans des groupes d'administration.

2 Installation et configuration initiale de l'Agent d'administration

L'Agent d'administration facilite la connexion de l'appareil au Serveur d'administration de Kaspersky Security Center. Il doit être installé sur chaque appareil qui sera connecté à Kaspersky Security Center.

1. Préparez vos appareils Linux pour l'installation de l'Agent d'administration. L'ensemble des actions nécessaires dépend du système d'exploitation.

2. Installez et effectuez la configuration initiale de l'Agent d'administration. Consultez l'aide de Kaspersky Security Center pour obtenir des instructions.

Par conséquent, les appareils sur lesquels l'Agent d'administration est installé s'affichent dans le groupe correspondant aux règles de déplacement configurées pour ces appareils. Si vous n'avez configuré aucune règle de déplacement, les appareils s'affichent dans le groupe **Appareils non définis**.

3 Installation du plug-in d'administration de Kaspersky Endpoint Security

Installez un plug-in d'administration de Kaspersky Endpoint Security en fonction de la console d'administration de Kaspersky Security Center que vous utilisez :

- Le **plug-in MMC d'administration de Kaspersky Endpoint Security** vous permet d'administrer le fonctionnement de l'application via la Console d'administration de Kaspersky Security Center. Le plugin MMC est installé sur l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center.

  Comment installer le plug-in MMC de Kaspersky Endpoint Security

  > Avant d'installer le plug-in MMC d'administration de Kaspersky Endpoint Security, il faut s'assurer que Kaspersky Security Center et Redist C ++ 2015 (Microsoft Visual C ++ 2015 Redistributable) sont installés.

  Pour installer le plug-in MMC :

  1. Téléchargez le fichier klcfginst.msi depuis la page de téléchargement des applications, dans la section **Kaspersky Endpoint Security for Linux** (**Version → Plug-in d'administration**).

  2. Sur l'appareil où est installée la Console d'administration de Kaspersky Security Center, exécutez le fichier klcfginst.msi.

  Après l'installation, le plug-in MMC d'administration s'affiche dans la liste des plug-ins MMC d'administration installés dans les propriétés du Serveur d'administration de Kaspersky Security Center.

  Pour afficher la liste des plug-ins MMC d'administration installés :

  1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le **nœud Serveur d'administration <nom du serveur>** et ouvrez la fenêtre des propriétés du Serveur d'administration de l'une des manières suivantes :

     - Ouvrez le menu contextuel du nœud **Serveur d'administration <nom du serveur>** et sélectionnez l'élément **Propriétés**.

     - Cliquez sur le lien **Propriétés du Serveur d'administration** dans la zone de travail du nœud **Serveur d'administration <nom du serveur>** de la section **Serveur d'administration**.

  2. Dans la liste de gauche, dans la section **Avancés**, sélectionnez la section **Informations sur les plug-ins d'administration installés des applications**.

     Dans la partie droite de la fenêtre, la liste des plug-ins d'administration installés affiche le plug-in MMC d'administration de Kaspersky Endpoint Security : **Kaspersky Endpoint Security <numéro de version> for Linux**.

  Si vous utilisez la Console d'administration de Kaspersky Security Center pour administrer l'application Kaspersky Endpoint Security et que plusieurs versions de l'application sont installées, vous devez installer un plug-in d'administration pour chaque version de l'application Kaspersky Endpoint Security. De cette façon, vous pourrez administrer l'application en utilisant des stratégies créées avec différentes versions du plug-in d'administration. Vous pouvez également convertir les stratégies et les tâches créées avec les versions précédentes du plug-in d'administration vers des versions plus récentes.

- le **plug-in Internet d'administration de Kaspersky Endpoint Security** vous permet de gérer l'application via Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console ; Le plug-in Internet est installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée. La fonctionnalité du plug-in Internet est disponible pour tous les administrateurs qui ont accès à Kaspersky Security Center Web Console dans un navigateur.

  Comment installer le plug-in Internet de Kaspersky Endpoint Security

  Vous pouvez installer le plug-in Internet de l'une des manières suivantes :

  - À l'aide de l'Assistant de configuration initiale de Kaspersky Security Center Web Console.

    Kaspersky Security Center Web Console vous invite automatiquement à exécuter l'assistant de configuration initiale lors de la première connexion de Kaspersky Security Center Web Console au Serveur d'administration. Vous pouvez également exécuter l'assistant de configuration initiale dans l'interface de Kaspersky Security Center Web Console (**Découverte et déploiement des appareils → Déploiement et attribution → Assistant de configuration initiale**). L'Assistant de configuration initiale de l'application peut également vérifier l'actualité des plug-ins Internet installés et charger les mises à jour indispensables. Pour en savoir plus sur l'Assistant de configuration initiale de Kaspersky Security Center Web Console, consultez l'aide de Kaspersky Security Center.

  - Manuellement, à l'aide d'un paquet de distribution provenant de la liste des plug-ins Internet de Kaspersky ou d'un fichier.

  Pour installer manuellement le plug-in Internet de Kaspersky Endpoint Security depuis Kaspersky Security Center :

  1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Configuration → Plug-ins Web**.

     Une liste des plug-ins Internet installés s'ouvrira.

  2. Cliquez sur le bouton **Ajouter**.

     La liste des plug-ins d'administration disponibles s'ouvre. La liste est mise à jour automatiquement lorsque de nouvelles versions de plug-ins Web sont publiées.

  3. Dans la liste des plug-ins disponibles, sélectionnez le plug-in Internet de **Kaspersky Endpoint Security <numéro de version> for Linux**.

  4. Dans la fenêtre qui s'ouvre avec une description du plug-in Web, cliquez sur le bouton **Installer le plug-in**.

  5. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

  Le nouveau plug-in s'affichera dans la liste des plug-ins Internet installés (**Configuration → Plug-ins Web**).

  Pour installer manuellement le plug-in Internet de Kaspersky Endpoint Security à partir d'un fichier :

  1. Téléchargez l'archive contenant le plug-in Internet depuis la page de téléchargement des applications, dans la section **Kaspersky Endpoint Security for Linux** (**Paquet de distribution complémentaire → Plug-in de la Web Console**).

  2. Décompressez localement l'archive téléchargée.

  3. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Paramètres → Plug-ins Web**.

     Une liste des plug-ins Internet installés s'ouvrira.

  4. Cliquez sur le bouton **Ajouter à partir d'un fichier**.

5. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez le chemin d'accès au fichier plugin.zip et le chemin d'accès au fichier signature.txt. Les fichiers se trouvent dans le dossier dans lequel vous avez décompressé l'archive contenant le plug-in Internet.

6. Cliquez sur le bouton **Ajouter**.

7. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in apparaît dans la liste des plug-ins Web installés (**Paramètres** → **Plug-ins Web**).

Si, dans les propriétés du Serveur d'administration de Kaspersky Security Center, vous avez sélectionné une langue qui n'est pas incluse dans le kit de distribution de l'application Kaspersky Endpoint Security, le Contrat de licence utilisateur final et toute l'interface de Kaspersky Security Center Web Console seront affichés en anglais.

Vidéo : Installation du plug-in Internet d'administration à l'aide de l'assistant



Vidéo : Installation du plug-in Internet d'administration dans les réseaux isolés



4 Création d'une stratégie Kaspersky Endpoint Security

Créez une stratégie pour Kaspersky Endpoint Security dans Kaspersky Security Center Web Console ou dans la Console d'administration (selon la console d'administration de Kaspersky Security Center que vous utilisez).

Gérez les paramètres suivants en fonction du mode dans lequel vous souhaitez utiliser l'application :

Pour le mode standard

Si vous avez créé une stratégie dans l'assistant de la Console d'administration, indiquez le mode d'utilisation de l'application : **Mode standard ou Mode Endpoint Detection and Response Agent**. Si vous avez créé une stratégie dans l'assistant de Kaspersky Security Center Web Console, ignorez la sélection du mode de l'application.

Pour le mode EDR Agent

1. Si vous avez créé une stratégie dans l'assistant de la Console d'administration, indiquez le mode d'utilisation de l'application : **Mode standard ou Mode Endpoint Detection and Response Agent**. Si vous avez créé une stratégie dans l'assistant de Kaspersky Security Center Web Console, ignorez la sélection du mode de l'application.

2. Terminez la création de la stratégie en suivant les instructions de l'assistant.

3. Ouvrez les propriétés de la stratégie créée dans Kaspersky Security Center Web Console ou dans la Console d'administration et activez l'intégration aux solutions Detection and Response que vous souhaitez utiliser pour protéger l'appareil :

   - Pour l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) sur la plateforme OSMP, vous devez activer et configurer le module EDR Expert (on-premises). Les paramètres sont disponibles dans Kaspersky Security Center Web Console

   - Pour l'intégration à Kaspersky Endpoint Detection and Response sur Kaspersky Anti Targeted Attack Platform, vous devez activer et configurer le module EDR Expert (on-premises). Les paramètres sont disponibles dans Kaspersky Security Center Web Console et dans la Console d'administration.

   - Pour l'intégration à Kaspersky Network Detection and Response sur Kaspersky Anti Targeted Attack Platform, vous devez activer et configurer le module NDR (KATA). Les paramètres sont disponibles dans Kaspersky Security Center Web Console et dans la Console d'administration.

Pour le mode Light Agent

Dans l'Assistant de création de la stratégie :

1. Indiquez le **mode Light Agent pour la protection des environnements virtuels**.

2. Gérez les paramètres de détection des SVM :

   a. Sélectionnez la méthode utilisée par les Light Agents pour détecter les SVM disponibles pour la connexion :

      - **Utiliser le Serveur d'intégration**. Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant.

      - **Utiliser la liste d'adresses des SVM définie manuellement**. Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

Si vous sélectionnez l'option **Utiliser la liste d'adresses des SVM définie manuellement**, que le Light Agent utilise l'algorithme avancé de sélection de la SVM et que le mode de protection des grandes infrastructures est activé sur une SVM, la connexion d'un Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez définir le paramètre **Emplacement des SVM** sur **Ignorer**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

b. Si vous avez sélectionné le Serveur d'intégration, la fenêtre de l'Assistant affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. Le cas échéant, indiquez de nouveaux paramètres de connexion : adresse IPv4 ou nom de domaine complet (FQDN) et port pour la connexion au Serveur d'intégration.

Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

c. Si vous sélectionnez une liste d'adresses SVM définie manuellement, créez une liste de SVM auxquelles les Light Agents administrés par cette stratégie peuvent se connecter. Pour ajouter une SVM à la liste, cliquez sur le bouton **Ajouter** et précisez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM dans la fenêtre qui s'ouvre. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application.

Pour les autres paramètres de la stratégie, vous pouvez conserver les valeurs par défaut. Les paramètres par défaut offrent un niveau de protection de base. Après l'installation de Kaspersky Endpoint Security, vous pouvez configurer la stratégie conformément aux exigences de votre organisation. Pour ce faire, vous pouvez utiliser les scénarios de configuration des modules de la section d'aide Administration de l'application.

Vidéo : création d'une stratégie



5 Configuration des mises à jour centralisées des bases et des modules de l'application

Par défaut, Kaspersky Endpoint Security est installé sur un appareil sans bases antivirus. L'application devient opérationnelle uniquement après le téléchargement des bases sur l'appareil. Pour que la protection commence immédiatement après l'installation de l'application, configurez les mises à jour centralisées des bases de données.

Dans Kaspersky Security Center Web Console ou dans la Console d'administration (selon la console d'administration de Kaspersky Security Center que vous utilisez) :

1. Lancez la tâche du Serveur d'administration *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. La tâche est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration.

   La tâche télécharge le paquet de mise à jour de Kaspersky Endpoint Security dans le répertoire des mises à jour sur le Serveur d'administration.

2. Créez une tâche de groupe de type *Mise à jour* pour l'application Kaspersky Endpoint Security. Dans les paramètres de la tâche, indiquez :

   - Source de mise à jour : Kaspersky Security Center.
   - Programmation de la tâche : au moins une fois par jour. Nous vous recommandons d'exécuter la tâche 4 à 6 fois par jour.

Vidéo : configuration des mises à jour centralisées des bases de données



6 Ajout de clés de licence et création d'une tâche d'activation

Pour activer l'application en mode standard, vous devez ajouter une clé de licence à l'application. Si certains modules ne sont pas couverts par votre licence, vous aurez peut-être besoin d'une autre clé de licence :

Pour activer l'application Kaspersky Endpoint Security en mode EDR Agent, vous avez besoin d'une clé de licence EDR Expert (on-premises).

Vous pouvez choisir une méthode d'activation en fonction de votre infrastructure et des exigences de votre organisation :

- Si l'application est installée sur tous vos appareils avec le même ensemble de fonctionnalités, utilisez la distribution automatique des clés de licence. La clé de licence à distribuer doit d'abord être ajoutée au stockage des clés de Kaspersky Security Center à l'aide d'un fichier clé ou d'un code d'activation. Pour en savoir plus, consultez l'Aide de Kaspersky Security Center.

- Si les ensembles de fonctionnalités de l'application diffèrent d'un appareil à l'autre, vous aurez besoin de clés de licence différentes pour l'activation. Dans ce cas, placez les appareils protégés dans différents groupes d'administration et configurez une tâche de groupe pour ajouter une clé pour chaque groupe d'administration.

Kaspersky Endpoint Security en mode Light Agent reçoit les informations sur la licence du Serveur de protection après la connexion à la SVM. Il n'est pas nécessaire d'activer séparément Kaspersky Endpoint Security en mode Light Agent.

Vidéo : activation de l'application à l'aide d'un code d'activation



Vidéo : activation de l'application à l'aide d'un fichier clé



Une fois Kaspersky Security Center préparé, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Installation de l'application.

Installation de l'application à l'aide de Kaspersky Security Center

Points particuliers à prendre en compte lors de l'installation :

- Le mode EDR Agent et le mode Light Agent de Kaspersky Endpoint Security ne sont pas pris en charge sur les appareils équipés d'un processeur Elbrus.
- Sur les appareils Arm, Kaspersky Endpoint Security en mode Light Agent n'est pas pris en charge.

Le scénario recommandé pour l'installation de l'application à l'aide de Kaspersky Security Center comprend les étapes suivantes :

Vous pouvez également installer l'application Kaspersky Endpoint Security via Kaspersky Security Center à l'aide de l'Assistant de démarrage rapide et de l'Assistant de déploiement de la protection.

1 Création du fichier d'installation

Le paquet d'installation de l'application Kaspersky Endpoint Security contient les éléments suivants :

- Le paquet de distribution principal
- Un paquet de distribution pour l'installation à distance de l'application
- Un paquet de distribution contenant l'interface graphique de l'application
- Paramètres de configuration initiale appliqués lors de l'installation

Vous pouvez créer un paquet d'installation des façons suivantes :

- **À partir d'un paquet de distribution hébergé sur les serveurs de Kaspersky**. Dans Kaspersky Security Center, un paquet d'installation est créé automatiquement à partir du paquet de distribution indiqué.

  Vidéo : création automatique d'un paquet d'installation dans Kaspersky Security Center



Pour installer l'application Kaspersky Endpoint Security sur des systèmes d'exploitation à prise en charge limitée (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), sélectionnez le paquet de distribution portant la mention `for legacy OS`.

- **Manuellement, à l'aide des fichiers préparés à l'étape Préparation des paquets de distribution**. Cette méthode est recommandée si vous souhaitez spécifier les paramètres de configuration initiale à l'aide d'un fichier de configuration ou si vous souhaitez utiliser le paquet d'installation créé avec différents systèmes d'exploitation ou différents gestionnaires de paquets.

  Vidéo : création manuelle d'un paquet d'installation dans Kaspersky Security Center

  Vous pouvez ajouter des bases de données de l'application préalablement téléchargées au paquet d'installation. Si un paquet d'installation avec des bases de données intégrées est utilisé pour l'installation, l'application est installée avec des bases de données fonctionnelles ; il n'est pas nécessaire de mettre à jour les bases de données immédiatement après l'installation.

Vous pouvez utiliser le même paquet d'installation à plusieurs reprises.

Comment préparer manuellement un paquet d'installation

1. Décompressez localement l'archive contenant les fichiers pour l'installation à distance de Kaspersky Endpoint Security.

2. Placez les paquets contenant les fichiers principaux de l'application dans le même répertoire.

   Si vous souhaitez utiliser le paquet d'installation créé avec différents systèmes d'exploitation ou gestionnaires de paquets, placez dans le répertoire les paquets de distribution correspondant à tous les types de systèmes d'exploitation et de gestionnaires de paquets dont vous avez besoin.

3. Si vous souhaitez utiliser l'interface graphique de l'application, placez les paquets de l'interface graphique dans le même répertoire.

   Activez l'utilisation de l'interface graphique en modifiant le paramètre approprié (`USE_GUI=Yes`) dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini. Par défaut, l'interface graphique n'est pas installée.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'interface utilisateur graphique n'est pas prise en charge.

4. Si vous souhaitez définir la configuration initiale de l'application à l'aide d'un fichier de configuration, ouvrez le fichier de configuration autoinstall.ini et modifiez-le si nécessaire. Le fichier autoinstall.ini se trouve dans le dossier dans lequel vous avez décompressé l'archive contenant les fichiers destinés à l'installation à distance de Kaspersky Endpoint Security.

   a. Par défaut, l'application est utilisée en mode standard.

      Pour utiliser l'application en mode EDR Agent, définissez `ENDPOINT_AGENT_MODE=Yes`.

      Pour utiliser l'application en mode Light Agent, définissez `KSVLA_MODE=Yes`.

      > Une fois Kaspersky Endpoint Security installé, il n'est pas possible de modifier le mode d'utilisation de l'application.

   b. Pour installer l'application en mode Light Agent :

      - Si vous installez l'application sur un modèle à partir duquel des machines virtuelles temporaires seront créées, définissez `VDI_MODE=Yes`. Ce paramètre active le mode de protection de l'infrastructure VDI pour optimiser les performances de l'application sur les machines virtuelles temporaires.

      - Spécifiez le rôle dans l'infrastructure virtuelle (serveur ou poste de travail) des machines virtuelles que vous souhaitez protéger (`SERVER_MODE=Yes|No`). Le rôle de la machine virtuelle détermine sous quelle licence l'application sera utilisée sur cette machine virtuelle et la quantité de fonctionnalités disponibles.

   Vous pouvez également modifier la configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé, sous l'onglet **Paramètres**.

5. Placez tous les fichiers préparés dans une archive ZIP, CAB, TAR ou TAR.GZ avec un nom arbitraire.

Comment créer un paquet d'installation dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez l'une des sections suivantes :

   - **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.

   - **Opérations → Stockages → Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

2. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création du paquet d'installation démarre.

3. Si vous utilisez la Web Console, sélectionnez la méthode de création du paquet d'installation :

   - **Générer un paquet d'installation à partir d'un fichier**. Le paquet d'installation sera créé à partir du fichier d'archive que vous avez préalablement préparé.

   - **Générer un paquet d'installation pour une application Kaspersky**. Le paquet d'installation sera créé à partir d'un distributif hébergé sur les serveurs de Kaspersky.

   Si vous utilisez Kaspersky Security Center Cloud Console, le paquet d'installation est créé à partir du paquet de distribution hébergé sur les serveurs de Kaspersky.

4. Selon la méthode de création du paquet :

   - Spécifiez le nom du paquet, cliquez sur le bouton **Parcourir** et indiquez le chemin d'accès à l'archive que vous avez préparée pour créer le paquet d'installation.

   - Sélectionnez la distribution de l'application Kaspersky Endpoint Security. Dans la fenêtre de droite, lisez les informations sur le paquet de distribution et cliquez sur le bouton **Télécharger et créer le paquet d'installation**. Le processus de création du fichier d'installation démarre.

5. Lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données. Avant de poursuivre la création du paquet d'installation, vous devez confirmer que vous avez lu le Contrat de licence utilisateur final et la Politique de confidentialité dans leur intégralité et que vous en acceptez les conditions.

6. Quittez l'Assistant.

   Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

7. Ouvrez les propriétés du paquet d'installation et accédez à l'onglet **Paramètres**.

   - Si vous installez l'application en mode EDR Agent, pour le paramètre **Mode d'utilisation**, sélectionnez **Endpoint Detection and Response Agent**.

   - Si vous installez l'application en mode Light Agent, spécifiez les paramètres suivants :

     Mode d'utilisation, sélectionnez l'option **Light Agent pour protéger les environnements virtuels**.

     Activer le mode de protection de l'infrastructure VDI. Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut.

     La machine virtuelle protégée est utilisée comme serveur. Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. Par défaut, la case est cochée (la machine virtuelle est utilisée dans l'infrastructure virtuelle comme serveur).

   - Si nécessaire, configurez les autres paramètres de configuration initiale.

     Pour obtenir une description de tous les paramètres de configuration initiale de l'application dans le paquet d'installation, consultez l'Annexe 1.

Comment créer un paquet d'installation dans la Console d'administration

Pour créer un paquet d'installation à l'aide de fichiers préparés :

1. Dans l'arborescence de la console, sélectionnez **Avancés** → **Installation à distance** → **Paquets d'installation**.

2. Cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du paquet d'installation démarre.

3. Cliquez sur le bouton **Créer un paquet d'installation pour l'application Kaspersky**.

4. Saisissez le nom du nouveau paquet d'installation, puis passez à l'étape suivante de l'Assistant.

5. Indiquez le chemin d'accès au fichier kesl.kud. Le fichier se trouve dans le dossier dans lequel vous avez décompressé l'archive contenant les fichiers d'installation de l'application (kesl.zip) à l'étape Préparation des paquets de distribution.

   La fenêtre affichera le nom et la version de l'application. Passez à l'étape suivante de l'Assistant.

6. Lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données.

   Pour continuer, confirmez que vous avez lu le Contrat de licence utilisateur final et la Politique de confidentialité dans leur intégralité et que vous en acceptez les conditions. Pour marquer votre accord, cochez les deux cases dans la fenêtre qui s'ouvre.

   Passez à l'étape suivante de l'Assistant.

7. L'Assistant charge les fichiers indispensables à l'installation de l'application sur le Serveur d'administration de Kaspersky Security Center. Attendez la fin du téléchargement et quittez l'Assistant.

8. Ouvrez les propriétés du paquet d'installation et accédez à l'onglet **Paramètres de l'application**.

   - Si vous installez l'application en mode EDR Agent, pour le paramètre **Mode d'utilisation de l'application**, sélectionnez **Endpoint Detection and Response Agent**.

   - Si vous installez l'application en mode Light Agent, spécifiez les paramètres suivants :

     Mode d'utilisation de l'application. Choisissez l'option **Light Agent pour protéger les environnements virtuels**.

     Activer le mode de protection de l'infrastructure VDI. Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut.

     La machine virtuelle protégée est utilisée comme serveur. Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. La case est cochée par défaut.

     Indisponible en mode Light Agent :

     - Configuration des sources de mise à jour des bases de données de l'application et lancement d'une mise à jour
     - Configuration du serveur proxy
     - Activation de l'application

     Après la connexion à la SVM, l'application en mode Light Agent reçoit les mises à jour des bases de données et les informations sur la licence du Serveur de protection. Il n'est pas nécessaire d'activer séparément Kaspersky Endpoint Security ni de configurer les mises à jour des bases de données.

   - Si nécessaire, configurez les autres paramètres de configuration initiale.

     Pour obtenir une description de tous les paramètres de configuration initiale de l'application dans le paquet d'installation, consultez l'Annexe 1.

   Vous pouvez configurer les paramètres de configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé dans la section **Paramètres de l'application**.

L'Assistant crée un paquet d'installation à partir du paquet de distribution provenant des serveurs de Kaspersky.

1. Dans l'arborescence de la console, sélectionnez **Avancés → Installation à distance → Paquets d'installation**.

2. Cliquez sur le bouton **Actions supplémentaires → Afficher les versions actuelles des applications de Kaspersky**.

3. Sélectionnez le paquet de distribution de Kaspersky Endpoint Security dans la liste, puis cliquez sur le bouton **Télécharger et créer un paquet d'installation**.

4. Lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données.

   Pour continuer, confirmez que vous avez lu le Contrat de licence utilisateur final et la Politique de confidentialité dans leur intégralité et que vous en acceptez les conditions. Pour confirmer, cochez les deux cases dans la fenêtre de confirmation, puis cliquez sur le bouton **Tout accepter**.

5. Attendez la fin du téléchargement. Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

6. Ouvrez les propriétés du paquet d'installation et accédez à la section **Paramètres de l'application**.

   - Si vous installez l'application en mode EDR Agent, pour le paramètre **Mode d'utilisation de l'application**, sélectionnez **Endpoint Detection and Response Agent**.

   - Si vous installez l'application en mode Light Agent, spécifiez les paramètres suivants :

     Mode d'utilisation de l'application. Choisissez l'option **Light Agent pour protéger les environnements virtuels**.

     Activer le mode de protection de l'infrastructure VDI. Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut.

     La machine virtuelle protégée est utilisée comme serveur. Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. La case est cochée par défaut.

     Les paramètres suivants ne sont pas disponibles en mode Light Agent :

     - Configuration des sources de mise à jour des bases de données de l'application et lancement d'une mise à jour
     - Configuration du serveur proxy
     - Activation de l'application

     Après la connexion à la SVM, l'application en mode Light Agent reçoit les mises à jour des bases de données et les informations sur la licence du Serveur de protection. Il n'est pas nécessaire d'activer séparément Kaspersky Endpoint Security ni de configurer les mises à jour des bases de données.

   - Si nécessaire, configurez les autres paramètres de configuration initiale.

     Pour obtenir une description de tous les paramètres de configuration initiale de l'application dans le paquet d'installation, consultez l'Annexe 1.

   Vous pouvez configurer les paramètres de configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé dans la section **Paramètres de l'application**.

2 Installation de l'application sur les appareils du réseau de l'entreprise

Vous pouvez installer l'application via Kaspersky Security Center à l'aide de la tâche d'installation à distance de l'application.

Si nécessaire, vous pouvez consulter le journal d'installation à distance de l'application à l'aide du diagnostic à distance de l'appareil client de Kaspersky Security Center.

La configuration initiale de l'application est effectuée automatiquement conformément aux paramètres définis dans les propriétés du paquet d'installation ou dans le fichier de configuration inclus dans le paquet d'installation.

Vidéo : installation, mise à jour des bases de données et vérification du fonctionnement de Kaspersky Endpoint Security



3 Mise à jour des bases de données de l'application

Si vous avez installé l'application en mode standard ou en mode EDR Agent, exécutez la tâche de groupe *Update* créée à l'étape « Configuration des mises à jour centralisées des bases de données et des modules de l'application » dans Web Console ou dans la Console d'administration (selon la console d'administration de Kaspersky Security Center que vous utilisez). Pour plus d'informations sur la mise à jour des bases de données de Kaspersky Endpoint Security, consultez la section Mise à jour des bases de données et des modules de l'application.

Si des mises à jour critiques sont reçues lors de la première mise à jour des bases de données et des modules dans les 24 heures suivant l'installation de l'application, celle-ci redémarre automatiquement.

4 Vérification de l'état de l'application

À l'issue de cette opération, l'application Kaspersky Endpoint Security a été installée et activée, et les bases de données de l'application ont été mises à jour. Après l'installation, l'application démarre automatiquement. Par défaut, les modules suivants sont activés :

- Protection contre les fichiers malicieux.
- Contrôle des appareils.
- Détection comportementale.

- Protection contre les menaces Internet : uniquement si l'un des navigateurs pris en charge est installé dans le système d'exploitation et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas installé dans les propriétés de la stratégie).

- Protection contre les menaces réseau : uniquement si les paramètres de la protection contre les menaces réseau sur l'appareil sont définis via une stratégie. Par défaut, la protection contre les menaces réseau est activée dans les propriétés de la stratégie. Si votre appareil utilise des paramètres configurés localement, la protection contre les menaces réseau est désactivée par défaut.

Vérifiez que l'application est prête à être utilisée.

Comment vérifier l'état de la protection d'un appareil dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

   La fenêtre des propriétés de l'appareil administré s'ouvre.

4. Dans l'onglet **Général**, sélectionnez la section **Protection**. Le champ **État de l'appareil** doit afficher *OK*.

   Si le champ **État de l'appareil** affiche des informations sur des droits insuffisants sur les répertoires système, vérifiez localement sur cet appareil les autorisations pour les répertoires suivants : /var/opt/kaspersky, /var/log/kaspersky et /opt/kaspersky. Assurez-vous que le propriétaire est root et que seul le propriétaire dispose d'un accès en écriture à ces répertoires.

5. Accédez à l'onglet **Applications**.

6. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

   La fenêtre des propriétés de l'application s'ouvrira.

7. Consultez **Bases de données de l'application** sous l'onglet **Général**, dans la section **Informations**. Assurez-vous que les bases de données de l'application sont à jour.

8. Accédez à la section **Licences** sous l'onglet **Général** et assurez-vous que l'application est activée.

9. Si vous avez installé l'application en mode EDR Agent, accédez à la section **Modules** sous l'onglet **Général** et assurez-vous que les intégrations que vous avez configurées à l'étape « Création d'une stratégie Kaspersky Endpoint Security » ont l'état *En cours d'exécution*.

10. Si vous avez installé l'application en mode Light Agent, accédez à la section **Modules** sous l'onglet **Général** et assurez-vous que la ligne **mode Light Agent pour la protection des environnements virtuels** affiche l'état *en cours d'exécution*. Cela signifie que l'application est utilisée en mode Light Agent.

Comment vérifier l'état de la protection d'un appareil dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

   La fenêtre des propriétés de l'appareil administré s'ouvre.

4. Sélectionnez la section **Protection**. Le champ **État de l'appareil** doit afficher *OK/Visible sur le réseau*.

   Si le champ **État de l'appareil** affiche des informations sur des droits insuffisants sur les répertoires système, vérifiez localement sur cet appareil les autorisations pour les répertoires suivants : /var/opt/kaspersky, /var/log/kaspersky et /opt/kaspersky. Assurez-vous que le propriétaire est root et que seul le propriétaire dispose d'un accès en écriture à ces répertoires.

5. Accédez à la section **Applications**.

6. Dans la liste des applications installées sur l'appareil, sélectionnez l'application Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application.

7. Consultez le champ **Bases de données de l'application** dans la section **Général**. Assurez-vous que les bases de données de l'application sont à jour.

8. Accédez à la section **Clés de licence** et vérifiez que l'application est activée.

9. Si vous avez installé l'application en mode EDR Agent, accédez à la section **Modules** et assurez-vous que les intégrations que vous avez configurées à l'étape « Création d'une stratégie Kaspersky Endpoint Security » ont l'état *En cours d'exécution*.

10. Si vous avez installé l'application en mode Light Agent, accédez à la section **Modules** et assurez-vous que la ligne **mode Light Agent pour la protection des environnements virtuels** affiche l'état *en cours d'exécution*. Cela signifie que l'application est utilisée en mode Light Agent.

Articles utiles

Que faire si les tâches ne s'exécutent pas ou si les stratégies ne sont pas appliquées

Que faire si l'appareil affiche l'état : « Paramètres de stratégie non valides. La stratégie n'a pas été appliquée. »

Erreur : « L'application n'est pas prise en charge par la version actuelle de Kaspersky Security Center Web Console ou le plug-in Internet de l'application n'est pas installé »

Résolution d'un problème lors de l'installation de l'interface graphique

Description des codes d'erreur d'installation

Erreurs après l'installation de Kaspersky Endpoint Security

Après avoir installé Kaspersky Endpoint Security, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Étapes de configuration supplémentaires après l'installation sur certains systèmes d'exploitation.

Installation de l'application à l'aide d'une ligne de commande

Points particuliers à prendre en compte lors de l'installation :

- Le mode EDR Agent et le mode Light Agent de Kaspersky Endpoint Security ne sont pas pris en charge sur les appareils équipés d'un processeur Elbrus.
- Sur les appareils Arm, Kaspersky Endpoint Security en mode Light Agent n'est pas pris en charge.
- Vous devez disposer des privilèges root pour installer l'application et l'interface graphique.
- L'Assistant de configuration initiale doit être exécuté avec les privilèges root.
- Si la version du gestionnaire de paquets apt est antérieure à 1.1.X, vous devez utiliser le gestionnaire de paquets dpkg (selon le système d'exploitation) pour effectuer l'installation.

Le scénario recommandé pour installer l'application à l'aide de la ligne de commande comprend les étapes suivantes :

1 Installation de l'application Kaspersky Endpoint Security

Avant de commencer l'installation, placez le paquet téléchargé contenant les fichiers principaux de l'application dans le répertoire /tmp de l'appareil.

Comment installer l'application à partir d'un paquet RPM

Sur un système d'exploitation 32 bits

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

Sur un système d'exploitation 64 bits

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

Sur un système d'exploitation ALT 64 bits

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

Sur un système d'exploitation 64 bits pour l'architecture Arm

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

Sur un système d'exploitation ALT 64 bits pour l'architecture Arm

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

Sur un système d'exploitation 64 bits pour l'architecture Elbrus

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

Sur un système d'exploitation ALT 64 bits pour l'architecture Elbrus

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

Sur un système d'exploitation 64 bits avec prise en charge limitée (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

Pour installer l'application sur CentOS 5.2, CentOS 5.4, CentOS 6.4 ou CentOS 6.6, vous devez télécharger sur le site le paquet de distribution portant la mention `OLD`.

Comment installer l'application à partir d'un paquet DEB

Sur un système d'exploitation 32 bits

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

Sur un système d'exploitation 64 bits

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

Sur un système d'exploitation 64 bits pour l'architecture Arm

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

Sur un système d'exploitation 64 bits pour l'architecture Elbrus

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

2 Installation de l'interface graphique de l'application

Si vous voulez administrer l'application à l'aide de l'interface graphique, vous devez installer l'interface graphique sur le même appareil que l'application.

Particularités de l'interface graphique de l'application :

- Vous ne pouvez pas installer l'interface graphique sur un appareil sur lequel l'application Kaspersky Endpoint Security n'est pas installée.
- Si l'application est utilisée en mode Light Agent, l'interface utilisateur graphique n'est pas prise en charge.

Avant de commencer l'installation, placez le paquet téléchargé contenant les fichiers de l'interface graphique de l'application dans le répertoire /tmp de l'appareil.

Comment installer l'interface graphique de l'application à partir d'un paquet RPM

Sur un système d'exploitation 32 bits

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

Sur un système d'exploitation 64 bits

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Sur un système d'exploitation ALT 64 bits

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Sur un système d'exploitation 64 bits pour l'architecture Arm

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Sur un système d'exploitation ALT 64 bits pour l'architecture Arm

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Sur un système d'exploitation 64 bits reposant sur l'architecture Elbrus

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

Sur un système d'exploitation ALT 64 bits reposant sur l'architecture Elbrus

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

Sur un système d'exploitation 64 bits avec prise en charge limitée (CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Pour installer l'application sur CentOS 6.4 ou CentOS 6.6, vous devez télécharger sur le site le paquet de distribution portant la mention OLD.

Comment installer l'interface graphique de l'application à partir d'un paquet DEB

Sur un système d'exploitation 32 bits

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

Sur un système d'exploitation 64 bits

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

Sur un système d'exploitation 64 bits pour l'architecture Arm

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

Sur un système d'exploitation 64 bits pour l'architecture Elbrus

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 Configuration initiale de l'application

Une configuration initiale est requise pour préparer l'application à l'utilisation et activer la protection de l'appareil client.

Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

La configuration initiale de l'application est effectuée à l'aide de l'Assistant de configuration initiale inclus dans le kit de distribution de Kaspersky Endpoint Security. Vous pouvez effectuer la configuration initiale en mode interactif ou en mode automatique.

Comment effectuer la configuration initiale de l'application en mode interactif.

Étape 1. Lancement de l'Assistant

Lancez l'Assistant de configuration initiale

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

À l'invite de l'Assistant, indiquez les valeurs des paramètres de configuration initiale de Kaspersky Endpoint Security étape par étape.

Si l'Agent d'administration est installé sur l'appareil et que vous installez l'application en mode standard ou en mode Agent EDR, vous pouvez ignorer les étapes de l'Assistant de configuration initiale relatives à la mise à jour des bases de l'application et à l'activation de l'application.

Étape 2. Sélection du mode standard ou du mode Light Agent

Saisissez `yes` pour utiliser l'application en mode Light Agent.

Saisissez `no` pour utiliser l'application en mode standard.

Si vous prévoyez d'utiliser l'application en mode Agent EDR, à cette étape, vous devez saisir `no` et sélectionner le mode Agent EDR à l'étape suivante.

Une fois la configuration initiale terminée, vous ne pouvez pas modifier la façon dont vous utilisez l'application.

Étape 3. Sélection du mode : standard ou Endpoint Detection and Response Agent

Cette étape s'affiche si vous avez choisi d'utiliser l'application en mode standard à l'étape 2.

Saisissez `yes` pour utiliser l'application en mode Agent EDR.

Saisissez `no` pour utiliser l'application en mode standard.

Une fois la configuration initiale terminée, vous ne pouvez pas modifier la façon dont vous utilisez l'application.

Étape 4. Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Cette étape s'affiche si vous avez choisi d'utiliser l'application en mode standard à l'étape 3.

Saisissez `yes` pour utiliser l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).

Saisissez `no` pour utiliser l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).

Étape 5. Sélection du rôle de la machine virtuelle

Cette étape s'affiche si vous avez choisi d'utiliser l'application en mode Light Agent à l'étape 2.

Spécifiez le rôle de la machine virtuelle (serveur ou poste de travail) sur laquelle vous installez Kaspersky Endpoint Security :

- Saisissez `yes` si vous utilisez une machine virtuelle comme serveur.
- Saisissez `no` si vous utilisez la machine virtuelle comme poste de travail.

Le rôle de la machine virtuelle détermine sous quelle licence l'application sera utilisée sur cette machine virtuelle et la quantité de fonctionnalités disponibles.

Étape 6. Activation du mode de protection de l'infrastructure VDI

Cette étape s'affiche si vous avez choisi d'utiliser l'application en mode Light Agent à l'étape 2.

Le mode de protection de l'infrastructure VDI vous permet d'optimiser le fonctionnement de Kaspersky Endpoint Security sur les machines virtuelles temporaires. Lorsque le mode de protection VDI est activé, les mises à jour nécessitant un redémarrage de la machine virtuelle ne sont pas installées. Lors de la réception de mises à jour nécessitant un redémarrage, le Light Agent installé sur une machine virtuelle envoie un message à Kaspersky Security Center concernant la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Saisissez `yes` si vous souhaitez activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de Kaspersky Endpoint Security sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées.

Saisissez `no` si vous ne souhaitez pas activer le mode de protection de l'infrastructure VDI. Recommandé si Kaspersky Endpoint Security est installé sur une machine virtuelle permanente ou sur un modèle de machine virtuelle à partir duquel des machines virtuelles permanentes seront créées.

Étape 7. Sélection des paramètres régionaux

À cette étape, l'Assistant affiche la liste des paramètres régionaux pris en charge au format défini dans la RFC 3066.

Spécifiez les paramètres régionaux tels qu'ils sont répertoriés ici. Cette norme sera utilisée :

- pour localiser les textes du Contrat de licence utilisateur final, de la Politique de confidentialité et de la Déclaration de Kaspersky Security Network, qui s'affichent lors de l'installation initiale ;
- pour la localisation des événements de l'application envoyés à Kaspersky Security Center.

La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.

Étape 8. Consultation du Contrat de licence utilisateur final et de la Politique de confidentialité

À cette étape, prenez connaissance du Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données.

Étape 9. Acceptation du Contrat de licence utilisateur final

Après avoir quitté le mode de consultation, saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions du Contrat de licence utilisateur final.
- `no` (ou `n`), si vous refusez les conditions du Contrat de licence utilisateur final.

Si vous avez refusé les conditions du Contrat de licence utilisateur final, la configuration de l'application Kaspersky Endpoint Security est interrompue.

Étape 10. Acceptation de la Politique de confidentialité

Après avoir quitté le mode de consultation, saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions de la Politique de confidentialité ;
- `no` (ou `n`), si vous refusez les conditions de la Politique de confidentialité.

Si vous avez refusé les conditions de la Politique de confidentialité, la configuration de l'application Kaspersky Endpoint Security est interrompue.

Étape 11. Utilisation de Kaspersky Security Network

À cette étape, acceptez ou refusez les conditions d'utilisation de Kaspersky Security Network :

- Saisissez `yes` (ou `y`) si vous acceptez les conditions générales de la Déclaration de Kaspersky Security Network. Le mode étendu de KSN sera activé.

- Saisissez `no` (ou `n`) si vous n'acceptez pas les conditions générales de la Déclaration de Kaspersky Security Network.

Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire /opt/kaspersky/kesl/doc/.

Le rejet de l'utilisation de Kaspersky Security Network n'entraîne pas l'arrêt de configuration initiale de l'application Kaspersky Endpoint Security. Vous pouvez activer, désactiver ou modifier le mode de Kaspersky Security Network à tout moment.

Si Kaspersky Security Network est activé, le mode Cloud est automatiquement activé ; dans ce mode, Kaspersky Endpoint Security utilise la version allégée des bases de données d'applications malveillantes.

Étape 12. Suppression des utilisateurs de groupes privilégiés

Cette étape s'affiche si des utilisateurs sont détectés dans le groupe kesladmin et/ou dans le groupe keslaudit.

Spécifiez si les utilisateurs doivent être supprimés des groupes privilégiés kesladmin et keslaudit. Les utilisateurs inclus dans les groupes kesladmin et keslaudit ont un accès privilégié aux fonctions de l'application.

Saisissez `yes` pour supprimer tous les utilisateurs détectés du groupe kesladmin et/ou keslaudit. Les utilisateurs dont le groupe primaire est kesladmin ou keslaudit seront déplacés vers le groupe nogroup. Si le groupe nogroup est manquant, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.

Saisissez `no` si vous ne souhaitez pas que l'application supprime les utilisateurs des groupes privilégiés.

Étape 13. Attribution du rôle d'administrateur à l'utilisateur

À cette étape, l'Assistant vous invite à attribuer le rôle d'administrateur (admin).

Saisissez le nom d'utilisateur auquel vous souhaitez attribuer le rôle d'administrateur. Le rôle d'administrateur est requise pour gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et via la ligne de commande de l'application sans utiliser la commande `sudo`.

Vous pouvez attribuer le rôle d'administrateur à un utilisateur ultérieurement, après avoir terminé la configuration initiale.

Étape 14. Configuration du mécanisme d'interception des événements système

L'application peut utiliser le mécanisme d'interception basé sur le module de noyau mis à jour si le système d'exploitation répond aux exigences liées à son installation. Si le système d'exploitation ne répond pas à ces exigences, mais prend en charge la technologie fanotify, l'application utilise fanotify pour intercepter les événements système. Si le système d'exploitation ne prend pas en charge la technologie fanotify, l'application compile et utilise un module de noyau spécial pour intercepter les événements système pour la Protection contre les fichiers malicieux. Si tous les paquets nécessaires sont installés, la compilation du module de noyau démarre automatiquement au lancement de la Protection contre les fichiers malicieux. Si les paquets nécessaires ne sont pas détectés sur l'appareil, l'application Kaspersky Endpoint Security proposera de les installer. En cas d'échec du téléchargement des paquets, un message d'erreur s'affiche.

- Saisissez `yes` si vous souhaitez utiliser le mécanisme d'interception basé sur le module de noyau mis à jour.
- Saisissez `no` si vous souhaitez utiliser le mécanisme d'interception système basé sur la technologie fanotify.

Si vous sélectionnez le mécanisme d'interception basé sur le module de noyau mis à jour, spécifiez les paramètres suivants :

- L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer :
  - Saisissez `yes` si vous souhaitez que l'application utilise la technologie fanotify pour intercepter les événements système si le module de noyau mis à jour ne parvient pas à démarrer.
  - Saisissez `no` si vous souhaitez que l'application continue de s'exécuter sans intercepter les événements système si le module de noyau mis à jour ne parvient pas à démarrer.

    Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

- Mode de redémarrage de l'application lors du passage à l'utilisation d'un module de noyau mis à jour. Pour exécuter le module, vous devez redémarrer l'application automatiquement ou manuellement.

  Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.

Saisissez `yes` pour autoriser le redémarrage automatique de l'application pour exécuter le module.

Étape 15. Activation de la configuration automatique de SELinux

Cette étape s'affiche si le système de contrôle d'accès SELinux est installé dans votre système d'exploitation.

Saisissez `yes` pour configurer automatiquement SELinux afin qu'il fonctionne avec Kaspersky Endpoint Security. Si l'application ne parvient pas à configurer automatiquement SELinux (par exemple, si l'utilitaire semanage est absent), l'Assistant affiche un message d'erreur et invite l'utilisateur à configurer SELinux manuellement.

Saisissez `no` si vous ne souhaitez pas exécuter la configuration automatique du système SELinux.

Par défaut, l'Assistant suggère `yes`.

Si nécessaire, vous pouvez configurer manuellement SELinux pour qu'il fonctionne avec l'application ultérieurement, après avoir terminé la configuration initiale de l'application.

Étape 16. Configuration de la source de mise à jour

Cette étape s'affiche si vous installez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR.

Indiquez la source de mise à jour pour les bases et modules d'application. Les bases de l'application contiennent les descriptions des signatures des menaces et les méthodes de lutte contre celles-ci. L'application utilise ces enregistrements pour rechercher et neutraliser les menaces. Les experts antivirus de Kaspersky ajoutent régulièrement des enregistrements sur les menaces.

Saisissez une des valeurs suivantes :

- `KLServers` : l'application récupère les mises à jour depuis un des serveurs de mise à jour de Kaspersky.
- `SCServer` : l'application télécharge les mises à jour sur l'appareil protégé depuis le serveur d'administration de Kaspersky Security Center installé dans votre organisation. Vous pouvez sélectionner cette source de mise à jour si vous utilisez l'application Kaspersky Security Center pour l'administration centralisée de la protection des appareils au sein de votre entreprise.
- `Custom` : l'application télécharge les mises à jour depuis la source personnalisée. Vous pouvez indiquer l'adresse d'une source de mise à jour personnalisée sous la forme d'un répertoire local (par exemple, /home/databases) ou d'un serveur HTTP ou HTTPS distant (par exemple, http://example.com/databases/).

Étape 17. Configuration des paramètres du serveur proxy

Cette étape s'affiche si vous installez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR.

Si vous utilisez un serveur proxy pour votre connexion Internet, saisissez l'adresse de votre serveur proxy dans l'un des formats suivants :

- `[<connection protocol>://]<address of proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ;
- `[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets.

  La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.

Si vous n'utilisez pas de serveur proxy, saisissez `no`.

Par défaut, l'application suggère `no`.

Vous pouvez configurer les paramètres du serveur proxy ultérieurement après avoir terminé la configuration initiale de l'application.

Étape 18. Démarrage d'une mise à jour de la base de données d'une application

Cette étape s'affiche si vous installez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR.

À cette étape, l'Assistant propose d'exécuter la tâche de mise à jour des bases de données de l'application sur l'appareil client immédiatement après l'installation.

Saisissez `no` si vous souhaitez refuser d'exécuter une mise à jour de la base de données de l'application.

Par défaut, l'Assistant suggère `yes`.

L'application Kaspersky Endpoint Security assure la protection de l'appareil uniquement après la mise à jour des bases de l'application.

Vous pouvez exécuter la tâche de mise à jour ultérieurement après avoir terminé la configuration initiale de l'application.

Étape 19. Activation de la mise à jour automatique des bases de l'application

Cette étape s'affiche si vous installez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR.

Saisissez `yes` pour activer la mise à jour automatique des bases de l'application. L'application recherche la présence éventuelle de mises à jour pour les bases toutes les 60 minutes par défaut. S'il existe des mises à jour, l'application télécharge les bases mises à jour.

Saisissez `no` si vous ne souhaitez pas que l'application mette à jour automatiquement les bases.

Vous pouvez activer les mises à jour automatiques de la base de données ultérieurement, après avoir terminé la configuration initiale de l'application, en planifiant la tâche de mise à jour.

Étape 20. Activation de l'application

Cette étape s'affiche si vous installez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR.

Si vous souhaitez activer l'application immédiatement après l'installation, saisissez un code d'activation ou indiquez le chemin d'accès complet au fichier clé.

Si vous n'avez pas indiqué de code d'activation ou de fichier clé, l'application sera activée avec une clé d'évaluation valide un mois.

Vous pouvez activer l'application ultérieurement après avoir terminé la configuration initiale de l'application.

Comment effectuer la configuration initiale en mode automatique

1. Créez un fichier de configuration contenant les paramètres de configuration initiale. Vous pouvez copier les paramètres du fichier de configuration autoinstall.ini, utilisé pour l'installation à distance de l'application à l'aide de Kaspersky Security Center, et les modifier si nécessaire.

2. Indiquez les paramètres obligatoires suivants dans le fichier de configuration :

   - Acceptation du Contrat de licence utilisateur final (CLUF) et de la Politique de confidentialité :

     ```
     EULA_AGREED=Yes
     PRIVACY_POLICY_AGREED=Yes
     ```

     Vous pouvez lire les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité dans le fichier license.<language ID> inclus dans le kit de distribution de l'application :

     Si vous n'acceptez pas les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, le processus d'installation est interrompu.

   - L'application Kaspersky Security Network est utilisée en mode standard par défaut.

Pour utiliser l'application en mode Agent EDR, indiquez le paramètre suivant :

```
ENDPOINT_AGENT_MODE=Yes
```

Pour utiliser l'application en mode Light Agent, indiquez le paramètre suivant :

```
KSVLA_MODE=Yes
```

- Utilisation de Kaspersky Security Network. Acceptez ou refusez les conditions d'utilisation de Kaspersky Security Network :

  ```
  USE_KSN=Yes|No
  ```

  Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire /opt/kaspersky/kesl/doc/. Si vous acceptez les conditions de la Déclaration de Kaspersky Security Network, le mode étendu de KSN est activé. Vous pouvez activer, désactiver ou modifier le mode de Kaspersky Security Network à tout moment.

  > Si Kaspersky Security Network est activé, le mode Cloud est automatiquement activé ; dans ce mode, Kaspersky Endpoint Security utilise la version allégée des bases de données d'applications malveillantes.

- Suppression automatique des utilisateurs des groupes privilégiés kesladmin et keslaudit avant l'installation de l'application :

  ```
  GROUP_CLEAN=Yes|No
  ```

3. Sélectionnez le mécanisme d'interception des événements système utilisé par Kaspersky Endpoint Security. Si vous souhaitez utiliser le module de noyau mis à jour pour intercepter les événements système, définissez la valeur :

   ```
   INTERCEPTOR_MODE=UseUpdatableKernelModule
   ```

   Par défaut, la technologie fanotify est utilisée pour intercepter les événements système.

4. Si vous installez l'application en mode standard ou en mode Agent EDR, indiquez les paramètres suivants :

   - Paramètres du serveur proxy. Si vous utilisez un serveur proxy pour votre connexion Internet, saisissez l'adresse de votre serveur proxy dans l'un des formats suivants :

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ;
     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets.

     > La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.

   - Installation et utilisation de l'interface graphique de l'application :

     ```
     USE_GUI=Yes|No
     ```

5. Si vous installez l'application en mode Light Agent, spécifiez les paramètres suivants :

   - Rôle de la machine virtuelle protégée :

     - `SERVER_MODE=Yes`, si la machine virtuelle protégée est utilisée comme serveur.

     - `SERVER_MODE=No`, si la machine virtuelle protégée est utilisée comme poste de travail.

   - Activation du mode de protection de l'infrastructure VDI pour optimiser les performances de l'application sur les machines virtuelles temporaires. Si vous installez l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées, définissez la valeur :

     `VDI_MODE=Yes`

6. Lancez l'Assistant de configuration initiale :

   ```
   /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
   ```

   où `<initial configuration file>` est le chemin d'accès au fichier de configuration contenant les paramètres de configuration initiale.

Lorsque l'Assistant de configuration initiale a terminé son exécution et que la console a été libérée, cela signifie que le processus de configuration initiale de l'application est terminé.

Vérification du code de retour

```
echo $?
```

Si la commande renvoie 0, la configuration post-installation de l'application est terminée avec succès.

Si des mises à jour critiques sont reçues lors de la première mise à jour des bases de données et des modules dans les 24 heures suivant l'installation de l'application, celle-ci redémarre automatiquement.

4 Vérification de l'état de l'application

À l'issue de cette opération, l'application Kaspersky Endpoint Security a été installée et activée, et les bases de données de l'application ont été mises à jour. Après l'installation, l'application démarre automatiquement. Par défaut, les modules suivants sont activés :

- Protection contre les fichiers malicieux.
- Contrôle des appareils.
- Détection comportementale.
- Protection contre les menaces Internet : uniquement si l'un des navigateurs pris en charge est installé dans le système d'exploitation et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas installé dans les propriétés de la stratégie).
- Protection contre les menaces réseau : uniquement si les paramètres de la protection contre les menaces réseau sur l'appareil sont définis via une stratégie. Par défaut, la protection contre les menaces réseau est activée dans les propriétés de la stratégie. Si votre appareil utilise des paramètres configurés localement, la protection contre les menaces réseau est désactivée par défaut.

Vérification de l'état de la protection de l'appareil en mode standard

Pour vérifier l'état de la protection de l'appareil, exécutez la commande suivante :

```
kesl-control --app-info [--json]
```

où `--json` signifie que les données sont affichées au format JSON. Si vous ne spécifiez pas la clé `--json`, les paramètres seront affichés dans la console.

Assurez-vous que :

- L'application est activée (ligne **Informations sur la licence de l'application**).
- Les bases de données de l'application sont à jour (lignes **Bases de l'application chargées** et **Date de la dernière publication des bases de données**).
- Le module Protection contre les fichiers malicieux est activé (ligne **Protection contre les fichiers malicieux**).
- La ligne **État de l'application** affiche `OK`.

  Si la ligne **État de l'application** affiche des informations sur des droits insuffisants sur les répertoires système, vérifiez localement sur cet appareil les autorisations pour les répertoires suivants : /var/opt/kaspersky, /var/log/kaspersky et /opt/kaspersky. Assurez-vous que le propriétaire est root et que seul le propriétaire dispose d'un accès en écriture à ces répertoires.

Vérification de l'état de la protection de l'appareil en mode EDR Agent

Pour vérifier l'état de la protection de l'appareil, exécutez la commande suivante :

```
kesl-control --app-info [--json]
```

où `--json` signifie que les données sont affichées au format JSON. Si vous ne spécifiez pas la clé `--json`, les paramètres seront affichés dans la console.

Assurez-vous que :

- L'application est activée (ligne **Informations sur la licence EDR Expert (on-premises)**)
- Les bases de données de l'application sont à jour (lignes **Bases de l'application chargées** et **Date de la dernière publication des bases de données**).
- L'application est utilisée en mode EDR Agent (ligne **Mode Endpoint Detection and Response Agent**).
- Pour les intégrations que vous avez configurées dans la stratégie, l'état « Available and running » est affiché.
- La ligne **État de l'application** affiche `OK`.

  Si la ligne **État de l'application** affiche des informations sur des droits insuffisants sur les répertoires système, vérifiez localement sur cet appareil les autorisations pour les répertoires suivants : /var/opt/kaspersky, /var/log/kaspersky et /opt/kaspersky. Assurez-vous que le propriétaire est root et que seul le propriétaire dispose d'un accès en écriture à ces répertoires.

Vérification de l'état de la protection de l'appareil en mode Light Agent

1. Exécutez la commande:

   ```
   kesl-control --ksvla-info
   ```

   Assurez-vous que l'application est utilisée en mode Light Agent (ligne **Mode Light Agent pour protéger les environnements virtuels**).

2. Si vous avez sélectionné un Serveur d'intégration dans la stratégie pour détecter les SVM disponibles pour la connexion, exécutez la commande suivante :

   ```
   kesl-control --viis-info
   ```

   Assurez-vous que Light Agent est connecté au Serveur d'intégration (ligne **État de la connexion au serveur d'intégration**).

3. Exécutez la commande:

   ```
   kesl-control --svm-info
   ```

   Assurez-vous que Light Agent est connecté à la SVM : des informations sur la SVM à laquelle une connexion est établie sont affichées.

4. Exécutez la commande:

   ```
   kesl-control --app-info [--json]
   ```

   où `--json` signifie que les données sont affichées au format JSON. Si vous ne spécifiez pas la clé `--json`, les paramètres seront affichés dans la console.

   Assurez-vous que :

   - Light Agent reçoit les informations sur la licence avec laquelle Kaspersky Security for Virtualization Light Agent est activé (ligne **Informations sur la licence de l'application**).
   - Les bases de données de l'application sont à jour (lignes **Bases de l'application chargées** et **Date de la dernière publication des bases de données**).
   - La ligne **État de l'application** affiche `OK`.

     Si la ligne **État de l'application** affiche des informations sur des droits insuffisants sur les répertoires système, vérifiez localement sur cet appareil les autorisations pour les répertoires suivants : /var/opt/kaspersky, /var/log/kaspersky et /opt/kaspersky. Assurez-vous que le propriétaire est root et que seul le propriétaire dispose d'un accès en écriture à ces répertoires.

Articles utiles

Que faire si les tâches ne s'exécutent pas ou si les stratégies ne sont pas appliquées

Que faire si l'appareil affiche l'état : « Paramètres de stratégie non valides. La stratégie n'a pas été appliquée. »

Erreur : « L'application n'est pas prise en charge par la version actuelle de Kaspersky Security Center Web Console ou le plug-in Internet de l'application n'est pas installé »

Résolution d'un problème lors de l'installation de l'interface graphique

Description des codes d'erreur d'installation

Erreurs après l'installation de Kaspersky Endpoint Security

Après avoir installé Kaspersky Endpoint Security, vous pouvez revenir au scénario de déploiement et continuer à partir de l'étape Étapes de configuration supplémentaires après l'installation sur certains systèmes d'exploitation.

Étapes de configuration supplémentaires après l'installation dans certains systèmes d'exploitation

Après la préparation de l'environnement en vue de l'installation de Kaspersky Endpoint Security et après l'installation de l'application, une configuration supplémentaire est requise pour certains systèmes d'exploitation.

Configuration de SELinux pour travailler manuellement avec l'application

Si votre système d'exploitation utilise le système de contrôle d'accès SELinux en mode `Enforcing`, il est automatiquement configuré par défaut pour fonctionner avec l'application pendant l'installation.

Si l'application ne parvient pas à configurer SELinux automatiquement (par exemple, si l'utilitaire semanage est manquant), l'Assistant affiche un message d'erreur et invite l'utilisateur à configurer SELinux manuellement. Dans ce cas, ou si vous avez refusé la configuration automatique, après avoir terminé la configuration initiale de l'application, configurez manuellement le système SELinux pour qu'il fonctionne avec l'application Kaspersky Endpoint Security.

> Cette configuration requiert les privilèges root.

Pour configurer manuellement le système SELinux pour qu'il fonctionne avec l'application :

1. Placez le système SELinux en mode non bloquant :
   - Si SELinux est activé, exécutez la commande suivante :

     ```
     setenforce Permissive
     ```

   - Si SELinux est désactivé, définissez `SELINUX=permissive` dans le fichier de configuration /etc/selinux/config, puis redémarrez le système d'exploitation.
2. Assurez que l'utilitaire semanage est installé dans le système. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.
3. Si vous utilisez une stratégie SELinux personnalisée plutôt que la stratégie par défaut 'targeted', attribuez une étiquette à chacun des fichiers exécutables d'origine de Kaspersky Endpoint Security conformément à votre stratégie SELinux.

   ```
   semanage fcontext -a -t bin_t <executable file>
   ```

```
restorecon -v <executable file>
```

Où `<executable file>` correspond à :

- /var/opt/kaspersky/kesl/<numéro de version_*>/opt/kaspersky/kesl/libexec/kesl
- /var/opt/kaspersky/kesl/<numéro de version_*>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/<numéro de version_*>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/<numéro de version_*>/opt/kaspersky/kesl/shared/kesl
- /var/opt/kaspersky/kesl/<numéro de version_*>/opt/kaspersky/kesl/bin/response

4. Lancez les tâches suivantes :

Exécuter la tâche Protection contre les fichiers malicieux

```
kesl-control --start-task 1
```

Exécuter la tâche Analyse des zones critiques

```
kesl-control --start-task 4 -W
```

Nous vous recommandons d'exécuter toutes les tâches de Kaspersky Endpoint Security que vous prévoyez d'exécuter à l'avenir.

5. Lancez l'interface utilisateur graphique si vous prévoyez de l'utiliser.

6. Assurez-vous que le fichier audit.log ne contient aucune erreur.

Afficher le fichier audit.log

```
grep kesl /var/log/audit/audit.log
```

7. Si vous découvrez des erreurs dans le fichier audit.log, créez et chargez un nouveau module de règles sur la base des enregistrements de blocage pour éliminer les erreurs, puis exécutez toutes les tâches que vous avez l'intention d'exécuter à l'avenir.

Créez et chargez un nouveau module de règles sur la base des enregistrements de blocage :

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

En cas d'apparition de nouveaux messages audit relatifs à Kaspersky Endpoint Security, il faut mettre à jour le fichier du module des règles.

8. Placez le système SELinux en mode bloquant.

```
setenforce Enforcing
```

Si vous utilisez une stratégie SELinux personnalisée, après l'installation des mises à jour de l'application, vous devez attribuer manuellement une étiquette aux fichiers exécutables d'origine de l'application Kaspersky Endpoint Security (suivez les étapes 1 et de 3 à 8).

Pour obtenir de plus amples informations, consultez la documentation du système d'exploitation utilisé.

Configuration de SELinux pour les actions de réponse

Si vous prévoyez d'utiliser SELinux en mode `Enforcing` sur votre système d'exploitation, vous devez gérer en outre les paramètres SELinux afin d'exécuter les actions de réponse lors de l'intégration avec les solutions Detection and Response.

Cette configuration SELinux requiert les privilèges root.

Pour configurer SELinux pour les actions de réponse :

1. Placez le système SELinux en mode non bloquant :

   - Si SELinux est activé, exécutez la commande suivante :

     ```
     Placez le système SELinux en mode non bloquant

     setenforce Permissive
     ```

   - Si SELinux est désactivé, définissez `SELINUX=permissive` dans le fichier de configuration /etc/selinux/config, puis redémarrez le système d'exploitation.

2. Assurez que l'utilitaire semanage est installé dans le système. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.

3. Exécutez toutes les tâches permettant d'effectuer les actions de réponse que vous souhaitez utiliser dans le cadre de l'intégration aux solutions Detection and Response.

4. Pour collecter des données d'investigation à l'aide des tâches Récupération d'une image mémoire et Récupération d'une image mémoire du processus, autorisez, dans SELinux, l'application Kaspersky Endpoint Security à accéder aux serveurs SMB indiqués dans les tâches.

5. Assurez-vous que le fichier audit.log ne contient aucune erreur.

   ```
   Afficher le fichier audit.log

   grep kesl /var/log/audit/audit.log
   ```

6. Si des erreurs sont présentes dans le fichier audit.log, créez et chargez un nouveau module de règles basé sur les enregistrements de blocage pour corriger les erreurs, puis exécutez à nouveau les tâches d'actions de réponse.

   ```
   Créez et chargez un nouveau module de règles sur la base des enregistrements de blocage :

   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

7. Placez le système SELinux en mode bloquant.

```
setenforce Enforcing
```

Configuration du lancement de l'application dans le système d'exploitation OSnova

Après avoir installé l'application, procédez comme suit pour lancer l'application :

1. Ouvrez le fichier `/etc/NESS/systemd/kesl.service.config` et définissez `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`.

2. Ouvrez le fichier `/etc/sysctl.d/30-disable-ptrace.conf` et définissez `kernel.yama.ptrace_scope=0`. D'autres valeurs du paramètre `kernel.yama.ptrace_scope` peuvent affecter le fonctionnement de l'application Kaspersky Endpoint Security ; pour plus de détails, consultez la section Problèmes connus et limitations.

3. Si vous souhaitez exécuter une analyse de la mémoire des processus et de la mémoire du noyau, vous devez désactiver le mécanisme de protection de la mémoire mprotect (ou PaX) dans le noyau. Pour ce faire, ajoutez l'option `mprotect=off` à la ligne de commande du noyau. Pour plus de détails, consultez la documentation OSnova.

4. Redémarrez le système d'exploitation.

Configuration du lancement de l'application sous ALT SP en mode environnement logiciel fermé

Après avoir installé l'application, procédez comme suit pour lancer l'application :

1. Définissez l'héritage du groupe kesl et des autorisations de répertoire pour les modules pouvant être mis à jour de Kaspersky Endpoint Security :

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. Définissez l'héritage du groupe kesl et des autorisations de répertoire pour les modules pouvant être mis à jour de l'Agent d'administration :

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. Activez le mode environnement logiciel fermé en lançant la signature du système :

```
integrity-applier -i -A
```

4. Assurez-vous que le sous-système IMA est activé :

```
cat /proc/cmdline
```

Le résultat de la commande doit contenir les lignes `lsm=integrity ima_hash=sha512 ima_appraise=enforce`.

5. Exécutez la tâche de mise à jour des bases de données :

```
kesl-control --start 6 -W
```

Si la sortie de la tâche de mise à jour des bases de données contient un événement *EventType=BasesApplied*, cela signifie que la mise à jour des bases de données a été effectuée correctement.

6. Redémarrez l'application :

```
systemctl restart kesl
```

Scénario de migration vers Kaspersky Security Center for Linux à l'aide du script d'installation rapide

Ce scénario comprend des exemples pour les cas d'utilisation suivants concernant la migration de la solution et de ses données vers un nouvel appareil doté du Serveur d'administration :

- Migration de Kaspersky Security Center Windows (MS SQL et PostgreSQL) vers Kaspersky Security Center Linux (PostgreSQL).
- Migration de Kaspersky Security Center Linux (PostgreSQL) dans le cadre d'un remplacement de matériel.

Le nouveau Serveur d'administration est déployé à l'aide du script d'installation rapide.

D'autres méthodes de transfert de données sont décrites dans la section consacrée à la migration vers Kaspersky Security Center Linux.

1 Conditions préalables à la création d'une copie de sauvegarde

Cette étape contient les instructions de préparation d'un Serveur d'administration précédemment configuré en vue d'une migration ultérieure vers un nouveau Serveur d'administration Kaspersky Security Center Linux. Le processus de préparation comprend les étapes suivantes :

1. Vérification de la version du Serveur d'administration afin de créer une copie de sauvegarde compatible avec Kaspersky Security Center Linux.

   Toutes les versions actuelles de **Kaspersky Security Center Linux** prennent en charge la migration des données avec une mise à jour de l'application vers une version plus récente. Les copies de sauvegarde peuvent être créées et restaurées uniquement dans le même type de SGBD.

Pour **Kaspersky Security Center Windows**, vous devez vérifier la version du Serveur d'administration dans **Propriétés** → **Général** → **Version**. Si la version est antérieure à 15.1.0.22239, mettez à jour Kaspersky Security Center Windows vers la dernière version.

Mise à jour de Kaspersky Security Center for Windows vers la dernière version.

1. Sur le site de Kaspersky, téléchargez le paquet de distribution correspondant à la langue de localisation du Serveur d'administration installé : `Version 15.1.0.22239 | Windows | Full distributive`.

   Le fichier exécutable est enregistré dans le dossier **Téléchargements** sous le nom suivant : `ksc_15.1_<build number>_full_<language>.exe`.

2. Copiez le paquet de distribution sur le Serveur d'administration.

3. Exécutez le fichier exécutable `ksc_15.1_<build number>_full_<language>.exe` en tant qu'administrateur.

4. Dans la fenêtre qui s'affiche, cliquez sur le lien **Installer Kaspersky Security Center**.

   L'Assistant d'installation du Serveur d'administration démarre.

5. Prenez connaissance des dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous acceptez toutes les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, dans la section **Je confirme que j'ai entièrement lu, que je comprends et que j'accepte les termes et les conditions de ce qui suit**, cochez les cases suivantes :

   - **Les termes et conditions de ce Contrat de licence utilisateur final**.
   - **La politique de confidentialité décrivant le traitement des données**.

6. Sélectionnez **Mettre à jour le Serveur d'administration et la console Web (recommandé)** et passez à l'étape suivante.

7. Créez une nouvelle copie de sauvegarde, sélectionnez l'option **Je souhaite créer une copie de sauvegarde des données** et suivez les étapes de l'Assistant de sauvegarde.

8. Cliquez sur **Mettre à jour**.

9. Pendant la mise à jour, dans l'Assistant d'installation de Web Console, confirmez toutes les étapes de mise à jour de la version.

   L'installation de la mise à jour du Serveur d'administration prendra un certain temps. Une fois l'Assistant d'installation terminé, la Console d'administration peut ne pas accepter de connexions tant que l'initialisation de la base de données n'est pas terminée.

10. Attendez la fin de la mise à jour.

2. Vérification de la conformité aux exigences relatives au certificat du Serveur d'administration.

   Avant de créer une copie de sauvegarde, vous devez vous assurer que le certificat contient le Subject Alternative Name (SAN). Si ce n'est pas le cas, veillez à remplacer le certificat, car sinon vous ne pourrez pas vous connecter à Web Console après une restauration à partir d'une copie de sauvegarde.

Pour vérifier que le certificat inclut l'autre nom de l'objet :

- Pour les appareils exécutant Windows :

  a. Dans la Console d'administration, sélectionnez le Serveur d'administration à vérifier.

  b. Dans le menu contextuel, sélectionnez **Propriétés** → **Général** → **Afficher le certificat du Serveur d'administration**.

  c. Une fenêtre s'ouvre ; dans celle-ci, vérifiez la valeur de l'élément **Autre nom de l'objet**.

- Pour un appareil Linux, exécutez la commande suivante :

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Assurez-vous que l'autre nom de l'objet contient le nom de domaine (DNS) de l'appareil sur lequel le Serveur d'administration est installé.

Si la valeur contient uniquement une adresse IP externe sans nom de domaine (DNS), ou si la valeur est complètement absente, remplacez manuellement le certificat par un certificat conforme aux exigences de Kaspersky Security Center Linux. Remplacez le certificat commun du Serveur d'administration à l'aide de l'utilitaire klsetsrvcert.

Remplacement du certificat commun du Serveur d'administration à l'aide de l'utilitaire klsetsrvcert

1. Créez un nouveau certificat avec une date de début différée sur les appareils en exécutant la commande suivante :

   - Pour Kaspersky Security Center Windows :

   ```
   "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
   <oldksc.example.internal>" -o "RsaKeyLen:2048"
   ```

   - Pour Kaspersky Security Center Linux :

   ```
   /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
   ```

   où `"<oldksc.example.internal>"` est le FQDN utilisé pour la connexion au Serveur d'administration.

   N'utilisez pas d'adresse IP pour cette valeur.

2. Définissez la date de début du nouveau certificat sur tous les appareils en exécutant la commande suivante :

   - Pour Kaspersky Security Center Windows :

   ```
   "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
   ```

   - Pour Kaspersky Security Center Linux :

   ```
   /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

où `"DD-MM-YYYY hh:mm"` est une date située au moins 30 jours après la date actuelle. Par défaut, la période de distribution d'un nouveau certificat (`CR`) est de 90 jours.

> Lorsque l'heure définie arrivera, vous devrez réinstaller Web Console afin de restaurer l'accès à celle-ci et de mettre à jour son certificat.

3. Si nécessaire, après la migration vers le nouveau Serveur d'administration, exécutez l'utilitaire klmover pour rétablir la connexion des appareils au Serveur d'administration. Vous devrez peut-être lancer cet utilitaire si un appareil est resté éteint pendant toute la période de distribution du certificat ou s'il ne s'est jamais connecté au Serveur d'administration.

2 Création d'une copie de sauvegarde de l'installation précédente du Serveur d'administration

Création d'une copie de sauvegarde de Kaspersky Security Center Windows

1. Depuis le **menu Démarrer** → **Kaspersky Security Center** → **Kaspersky Backup Utility**, exécutez l'utilitaire `klbackup.exe` qui se trouve dans le dossier d'installation de Kaspersky Security Center Linux.

   L'Assistant d'installation de l'application sera lancé. Sous Microsoft Windows en mode Server Core, utilisez la version console de l'utilitaire klbackup.

2. À la première étape, sélectionnez **Effectuer une sauvegarde des données du Serveur d'administration**.

3. À l'étape **Paramètres de sauvegarde** :

   a. Cliquez sur le bouton **Parcourir** et créez un nouveau dossier pour enregistrer la copie de sauvegarde séparément du répertoire par défaut, par exemple `C:\kscbackups`.

   b. Si vous utilisez Microsoft SQL Server, sélectionnez l'option **Migrer la base de données** → **Migrer vers Postgres** pour l'utiliser avec le script d'installation rapide. Lors du déploiement de Kaspersky Security Center Linux selon la méthode standard, vous pouvez également migrer les données vers une base de données MySQL/MariaDB.

   c. Définissez un mot de passe pour la copie de sauvegarde afin de la protéger contre tout accès non autorisé aux données.

4. Attendez que la copie de sauvegarde soit créée et quittez l'utilitaire.

Un nouveau sous-répertoire portant l'horodatage de la sauvegarde est créé dans le répertoire spécifié.

Création d'une copie de sauvegarde de Kaspersky Security Center Linux

1. Sur l'appareil du Serveur d'administration, exécutez la commande suivante en ligne de commande :

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Attendez la fin du processus de sauvegarde.

Un nouveau sous-répertoire portant l'horodatage de la sauvegarde est créé dans le répertoire spécifié dans l'option `-path`.

Après avoir créé une copie de sauvegarde de votre ancien Serveur d'administration, mettez hors service l'appareil du Serveur d'administration.

Mise hors service de l'appareil du Serveur d'administration

1. Copiez sur l'appareil de l'administrateur la copie de sauvegarde obtenue pour la migration des données.
2. Arrêtez le système d'exploitation du Serveur d'administration.
3. Débranchez la carte réseau du réseau d'entreprise.
4. Libérez l'adresse IP de l'appareil si vous prévoyez de la réutiliser pour la nouvelle installation de Kaspersky Security Center Linux.
5. Assurez-vous que l'appareil est complètement hors tension.

La présence de l'ancien Serveur d'administration sur le réseau peut provoquer des dysfonctionnements de l'administration des appareils et perturber le processus de connexion à la Web Console du nouveau Serveur d'administration, ainsi qu'entraîner le lancement de la tâche d'installation de l'Agent d'administration avec une connexion à l'ancien serveur.

3 Déploiement initial de Kaspersky Security Center Linux à l'aide du script d'installation rapide

Ce guide décrit le déploiement initial d'une instance de Kaspersky Security Center Linux à l'aide du script d'installation rapide.

Considérations particulières :

- Tous les modules de Kaspersky Security Center sont installés sur le même appareil que le Serveur d'administration.
- Le système d'exploitation du Serveur d'administration doit être l'un des suivants :
  - Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8.5) avec PostgreSQL 15
  - Ubuntu Server 26.04 LTS avec PostgreSQL 18
  - CentOS Stream 10 avec PostgreSQL 18
  - RED OS 8.0 avec PostgreSQL 16
- Le script d'installation rapide automatise uniquement la configuration et l'installation de l'application Kaspersky Security Center. L'administrateur doit prendre des mesures pour configurer le nom de l'appareil du Serveur d'administration dans le système d'exploitation, les cartes réseau et les pare-feu de sécurité au niveau du système d'exploitation, ainsi que le matériel.

Le déploiement initial d'une instance de Kaspersky Security Center Linux à l'aide du script d'installation rapide comprend les étapes suivantes :

1. Préparation du déploiement

Avant de procéder aux étapes d'installation, vous devez préparer les éléments suivants :

- Une image disque d'installation du système d'exploitation et un référentiel de paquets d'applications.
- Une application d'authentification pour l'authentification à deux facteurs (2FA) lors de la connexion à la Web Console.
- Un nouveau FQDN (par exemple, *ksclinux.example.com*). Si vous disposez d'une expérience suffisante en matière de configuration de solutions, vous pouvez utiliser votre propre script pour attribuer le FQDN précédent au nouveau serveur lors de l'installation. Dans ce cas, à l'étape 5, « Configuration de l'application après la restauration à partir d'une copie de sauvegarde », ignorez l'étape 4. Restauration de la connexion des appareils administrés au FQDN du Serveur d'administration précédent
- Appareil de l'administrateur doté d'un navigateur pour télécharger les distributions et administrer la Web Console via Internet.
- Assurez la disponibilité du DNS et d'un serveur de temps (NTP) pour les modules de l'application.
- En fonction de votre scénario, libérez l'ancienne adresse IP si elle était utilisée pour connecter les appareils administrés.
- Configurez l'équipement réseau et le serveur proxy conformément aux exigences suivantes :
  - Ports de communication entre les modules de l'application.
  - Accès aux serveurs de Kaspersky.
  - Recommandations du guide de renforcement.

2. Dimensionnement et configuration du système d'exploitation

1. Configurez l'équipement en fonction du nombre d'appareils que le Serveur d'administration va gérer.

   Chaque calcul de dimensionnement tient compte des ressources disponibles pour les applications Kaspersky. Le calcul tient compte du Serveur d'administration, de l'Agent d'administration, du SGBD, du Web Console Server et de Kaspersky Endpoint Security for Linux, qui fonctionnent tous sur le même appareil. Cependant, le calcul ne tient pas compte du stockage des copies de sauvegarde du Serveur d'administration.

   > Utilisez un partage de fichiers externe comme point de montage pour stocker les copies de sauvegarde sur un appareil distinct ou augmentez l'exigence en matière d'espace libre sur le disque dur en tenant compte du stockage des sauvegardes.

   Nous vous recommandons d'ajouter 4 à 6 Go de RAM et 20 Go d'espace libre sur le disque dur pour le système d'exploitation.

   Dimensionnement de l'appareil en fonction du nombre d'appareils administrés :

   - **S** (jusqu'à 1 000 appareils) : 8 cœurs de processeur, 16 Go de RAM, 70 Go d'espace libre sur le disque dur pour le répertoire `/var`, 300 IOPS ou plus.
   - **M** (jusqu'à 10 000 appareils) : 12 cœurs de processeur, 24 Go de RAM, 340 Go d'espace libre sur le disque dur pour le répertoire `/var`, 300 IOPS ou plus.

- **L** (jusqu'à 30 000 appareils) : 20 cœurs de processeur, 40 Go de RAM, 490 Go d'espace libre sur le disque dur pour le répertoire `/var`, 300 IOPS ou plus.

- **XL** (jusqu'à 50 000 appareils) : 28 cœurs de processeur, 54 Go de RAM, 640 Go d'espace libre sur le disque dur pour le répertoire `/var`, 300 IOPS ou plus.

2. Préparez le matériel du serveur Kaspersky Security Center conformément aux spécifications sélectionnées.

3. Installez le système d'exploitation sur le serveur Kaspersky Security Center.

   Pendant l'installation, activez l'option **Outils de connexion à distance SSH** si vous prévoyez d'administrer à distance l'appareil doté du Serveur d'administration via la ligne de commande.

   > Astra Linux doit être installé avec l'option **Contrôle d'accès obligatoire** désactivée. En outre, pour que Kaspersky Endpoint Security for Linux fonctionne correctement, désactivez l'option **Bloquer le traçage ptrace**.

4. Vérifiez l'espace disque disponible pour le répertoire `/var` s'il est monté séparément, ou pour le répertoire racine `/`.

   Exemples pour une configuration M :

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. Configurez l'adresse IP du Serveur d'administration précédent sur le nouveau serveur si une adresse IP était utilisée pour connecter les appareils gérés.

Vidéo : configuration du système d'exploitation



3. Téléchargement des fichiers de distribution

1. Téléchargez les paquets de distribution depuis le site de Kaspersky et enregistrez-les dans un répertoire distinct (par exemple, *kscdistr*).

   Pour Ubuntu et Astra Linux

   - Paquet de distribution du Serveur d'administration au format .deb :
     `Version 16.3.0.1207 | Debian x64 | Administration server`
   - Paquet de distribution de Web Console au format .deb :
     `Version 16.3.0.1207 | Debian x64 | Web console`
   - Script d'installation rapide :
     `Version 16.3.0.1207 | Linux | KSC installation script`

   Pour CentOS et RED OS

   - Paquet de distribution du Serveur d'administration au format rpm :
     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`
   - Paquet de distribution de Web Console au format rpm :
     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`
   - Script d'installation rapide :
     `Version 16.3.0.1207 | Linux | KSC installation script`

2. Pour permettre aux applications Kaspersky de fonctionner en mode d'environnement logiciel fermé d'Astra Linux, téléchargez le fichier de clé publique kaspersky_astra_pub_key.gpg.

3. Copiez les fichiers téléchargés sur le nouvel appareil doté du Serveur d'administration de Kaspersky Security Center à l'aide d'un support amovible ou via le réseau.

   Voici les actions à effectuer pour copier les fichiers via le réseau à l'aide de la ligne de commande.

   > La possibilité d'utiliser l'utilitaire scp pour copier les fichiers dépend de l'exécution d'un service SSH dans le système d'exploitation de l'appareil du Serveur d'administration, ainsi que de la stratégie de sécurité de votre organisation.

   a. Dans la ligne de commande, utilisez la commande cd pour accéder au répertoire situé un niveau au-dessus du répertoire *kscdistr*, par exemple :

   Pour Linux

   ```
   cd /home/administrator/Desktop
   ```

   Pour Windows

   ```
   cd C:\Users\Administrator\Downloads
   ```

b. Copiez les fichiers de distribution via le réseau à l'aide de l'utilitaire scp :

```
scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
```

où :

Le répertoire `<kscdistr>` est le répertoire local contenant les paquets de distribution téléchargés de Kaspersky Security Center.

`<administrator>` est un superutilisateur du nouveau Serveur d'administration autorisé à utiliser une connexion SSH.

`<ksclinux.example.com>` est l'adresse FQDN du nouveau Serveur d'administration.

Les fichiers sont copiés à la racine du répertoire de base de l'utilisateur spécifié.

4. Configuration des paramètres d'installation

1. Sur l'appareil doté du nouveau Serveur d'administration, connectez-vous en tant que superutilisateur et ouvrez un terminal.

2. Accédez au répertoire contenant les paquets de distribution copiés.

Exemple

```
cd ~/kscdistr
```

3. Extrayez l'archive du script d'installation rapide dans le répertoire actuel contenant les fichiers de distribution.

Exemple

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Vérifiez la présence de tous les fichiers à l'aide de la commande suivante :

```
ls -la
```

Exemple de sortie de la commande ls -la

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. Dans le répertoire contenant les distributions, ouvrez le fichier texte contenant les paramètres du script d'installation pour le modifier, par exemple :

```
nano ./params.txt
```

6. Définissez les valeurs préparées précédemment et supprimez le premier caractère de commentaire (#) dans les lignes concernées, ou ajoutez de nouvelles lignes contenant les valeurs suivantes :

   - Dimensionnement de l'équipement (valeurs pour les configurations S/M/L/XL).

     Exemple

     ```
     klfi_netsize=S
     ```

   - Adresse FQDN du Serveur d'administration dans deux paramètres du fichier.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

   La langue du Serveur d'administration installé dépend des paramètres régionaux du paquet de distribution téléchargé.

7. Vérifiez que le FQDN du Serveur d'administration est correctement résolu en adresse IP de bouclage dans le système d'exploitation du nouveau Serveur d'administration. Pour ce faire, procédez comme suit :

   a. Exécutez la commande `ping` avec l'adresse du nouveau Serveur d'administration.

      Exemple d'obtention réussie d'une adresse IP de bouclage

      ```
      administrator@ksclinux:~$ ping ksclinux.example.com
      ping ksclinux.example.com
      PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
      64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
      ```

   b. Ajoutez l'adresse du Serveur d'administration au fichier `/etc/hosts` du système d'exploitation sur le nouveau Serveur d'administration si aucune adresse n'a été obtenue ou si une adresse IP externe a été obtenue.

      Pour ce faire, procédez comme suit :

      - Ouvrez le fichier `/etc/hosts` pour le modifier en exécutant la commande suivante :

        ```
        sudo nano /etc/hosts
        ```

      - Saisissez l'adresse du serveur sous forme de FQDN de l'appareil doté du Serveur d'administration, par exemple :

        ```
        127.0.0.1       localhost
        127.0.1.1       ksclinux.example.com ksclinux
        <...>
        ```

   Sur les appareils administrés, le FQDN du Serveur d'administration doit être résolu en adresse IP externe du serveur. Assurez-vous que les enregistrements sur les serveurs DNS sont correctement configurés.

5. Démarrage du script d'installation rapide

Pour exécuter le script d'installation rapide :

1. Après le redémarrage de l'appareil, retournez dans le répertoire contenant les paquets de distribution :

   ```
   cd ~/kscdistr
   ```

2. Rendez le fichier exécutable en exécutant la commande suivante :

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. Lisez les Contrats de licence utilisateur final dans la langue de votre version localisée avant d'exécuter le script, car le script d'installation rapide lui-même est disponible uniquement en anglais.

4. Connectez les dépôts de paquets réseau au système d'exploitation ou à l'image du disque d'installation du système d'exploitation afin que les paquets puissent être téléchargés pendant l'installation.

5. Exécutez le script d'installation rapide :

   ```
   sudo ./ksc_fast_install.py
   ```

6. Suivez les étapes de l'Assistant d'installation.

   Si le script indique à tort que vous ne disposez pas de suffisamment de RAM à l'étape de vérification des ressources, désactivez l'allocation dynamique de RAM pendant l'installation.

7. Attendez la fin de l'installation. Dans le texte de sortie du script, enregistrez le nom d'utilisateur (`User`) et le mot de passe (`Pass`) pour la Web Console.

   Exemple

   ```
   [+] Creating KSC user 'kscadmin' ...
   [+] An internal user has been created:
   [+]     User: kscadmin
   [+]     Pass: ############
   [!] If the password is lost, you must create a user by running the command:
           /opt/kaspersky/ksc64/sbin/kladduser -n <user>
   [+] OK
   [+] Success
   ```

Vidéo : exécution du script d'installation rapide pour Ubuntu



6. Première connexion à la Web Console

1. Dans un navigateur, ouvrez l'adresse de la Web Console : `https://<FQDN>:8080`

   où `<FQDN>` est l'adresse du Serveur d'administration indiquée dans les paramètres du script d'installation, par exemple *https://ksclinux.example.com:8080*.

2. Connectez-vous à la Web Console à l'aide du nom d'utilisateur et du mot de passe indiqués dans la sortie du script.

3. Configurez l'application d'authentification :

   a. Copiez la clé secrète permettant d'obtenir des codes de confirmation à usage unique dans l'application ou scannez le code QR depuis l'Assistant d'authentification de la Web Console.

   b. Saisissez le code de confirmation généré pour vous authentifier et vous connecter à la Web Console.

4. Consultez le Guide de durcissement et confirmez-en la prise de connaissance.

5. Configurez le Serveur d'administration dans l'Assistant de configuration initiale si vous ne comptez pas restaurer les données du Serveur d'administration à partir d'une copie de sauvegarde.

4 Restauration d'une copie de sauvegarde du Serveur d'administration

Dans les scénarios de migration depuis Kaspersky Security Center Windows ou de migration des données de Kaspersky Security Center Linux vers un nouveau matériel, vous devrez peut-être restaurer les données à partir d'une copie de sauvegarde créée dans l'ancienne installation du Serveur d'administration.

La version de PostgreSQL sur le nouveau serveur doit au moins correspondre à celle contenue dans la copie de sauvegarde.

Ignorez cette étape si vous n'avez pas besoin de restaurer les données.

Si aucune copie de sauvegarde n'a été créée auparavant :

- Créez une copie de sauvegarde de l'ancienne installation du Serveur d'administration avec le type de format de données PostgreSQL.
- Installez un nouveau serveur Kaspersky Security Center Linux et connectez-vous à la Web Console pour la première fois.

La restauration du Serveur d'administration à partir d'une copie de sauvegarde comprend les étapes suivantes :

1. Placement de la copie de sauvegarde sur le Serveur d'administration

Placez la copie de sauvegarde de l'ancien Serveur d'administration sur l'appareil du nouveau Serveur d'administration à l'aide d'un support amovible ou du réseau.

Pour copier la copie de sauvegarde sur le Serveur d'administration via le réseau :

> La possibilité d'utiliser l'utilitaire scp pour copier les fichiers dépend de l'exécution d'un service SSH dans le système d'exploitation de l'appareil du Serveur d'administration, ainsi que de la stratégie de sécurité de votre organisation.

1. Dans la ligne de commande, utilisez la commande *cd* pour accéder au répertoire contenant les fichiers de sauvegarde du Serveur d'administration précédent, par exemple :

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Copiez le répertoire contenant les fichiers de sauvegarde à l'aide de l'utilitaire scp :

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   où :

   `<klbackup202x-xx-xx>` est le répertoire dans lequel les fichiers de sauvegarde sont stockés.

   `<administrator>` est un superutilisateur du nouveau Serveur d'administration autorisé à utiliser une connexion SSH.

   `<ksclinux.example.com>` est l'adresse FQDN du nouveau Serveur d'administration.

Le répertoire contenant la copie de sauvegarde est copié dans le répertoire de base de l'utilisateur indiqué.

2. Procédure de restauration à partir d'une sauvegarde

1. Sur l'appareil du nouveau Serveur d'administration, ouvrez le terminal.
2. Lors de la restauration des données à partir d'une copie de sauvegarde, accordez les droits de superutilisateur PostgreSQL aux comptes standard klserver et kliam que le Serveur d'administration utilise pour se connecter à la base de données :

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Utilisez l'utilitaire klbackup pour lancer la restauration des données à partir de la copie de sauvegarde de l'ancien Serveur d'administration :

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   où `</home/administrator/klbackup202x-xx-xx>` est le chemin d'accès complet au répertoire contenant les fichiers de sauvegarde.

4. Si aucun mot de passe n'a été défini pour la sauvegarde, appuyez sur **Entrée** sans saisir de mot de passe lorsque vous êtes invité à saisir le mot de passe de la sauvegarde.
5. Attendez la fin de l'exécution de l'utilitaire.

   Pour les installations de grande taille, l'opération peut prendre beaucoup de temps.

6. Rétablissez les autorisations d'origine pour les comptes PostgreSQL que le Serveur d'administration utilise pour se connecter à la base de données.

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
   ```

5 Configuration de l'application après la restauration à partir d'une copie de sauvegarde

Ignorez cette étape si vous n'avez pas restauré les données à partir d'une copie de sauvegarde.

La configuration de l'application après la restauration à partir d'une copie de sauvegarde comprend les étapes suivantes :

1. Restauration de la Web Console

1. Récupérez l'adresse de l'ancien serveur dans le fichier de configuration du Serveur IAM :

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Exemple

```
ksc_address: "oldksc.example.internal"
```

2. Vérifiez si le FQDN de l'ancien Serveur d'administration est correctement résolu en adresse IP de bouclage du nouveau Serveur d'administration. Pour ce faire, procédez comme suit :

   a. Exécutez la commande `ping` avec l'adresse de l'ancien Serveur d'administration.

Exemple d'obtention réussie d'une adresse IP de bouclage

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Ajoutez l'adresse du Serveur d'administration au fichier `/etc/hosts` du système d'exploitation sur le nouveau Serveur d'administration si aucune adresse n'a été obtenue ou si une adresse IP externe a été obtenue. Pour ce faire, procédez comme suit :

   - Ouvrez le fichier /etc/hosts pour le modifier :

```
sudo nano /etc/hosts
```

   - Saisissez le nom de l'ancien serveur comme alias supplémentaire pour l'adresse de l'appareil du Serveur d'administration.

Exemple

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Réinstallez la Web Console :

   a. Désinstallez le serveur Web Console local :

   Selon le paquet de distribution de Kaspersky Security Center Linux, exécutez l'une des commandes suivantes :

   - Sur un système d'exploitation basé sur Debian :

```
sudo apt remove ksc-web-console -y
```

   - Sur un appareil exécutant un système d'exploitation basé sur Red Hat Enterprise Linux :

```
sudo dnf remove ksc-web-console -y
```

b. Installez le paquet de la Web Console depuis le répertoire contenant les paquets de distribution :

- Sur un système d'exploitation basé sur Debian :

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- Sur un appareil exécutant un système d'exploitation basé sur Red Hat Enterprise Linux :

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2. Restauration de l'accès de l'utilisateur kscadmin lors de la migration depuis Kaspersky Security Center Windows

La base de données des utilisateurs a été écrasée ; recréez l'utilisateur kscadmin et configurez l'authentification à deux facteurs.

1. Ouvrez le terminal dans le système d'exploitation de l'appareil du Serveur d'administration et exécutez la commande suivante pour créer un utilisateur :

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   Après avoir appuyé sur **Entrée**, saisissez un mot de passe, puis saisissez-le à nouveau.

2. Dans un navigateur, ouvrez l'adresse de la Web Console :

   ```
   https://<FQDN>:8080
   ```

   où `<FQDN>` est l'adresse du Serveur d'administration indiquée dans les paramètres du script d'installation, par exemple *https://ksclinux.example.com:8080*.

3. Utilisez le nom d'utilisateur et le mot de passe créés pour vous connecter à la Web Console.

4. Configurez l'application d'authentification. Pour ce faire, procédez comme suit :

   a. Supprimez l'ancien profil utilisateur kscadmin de l'application d'authentification avant de restaurer la copie de sauvegarde du Serveur d'administration.

   b. Copiez la clé secrète permettant d'obtenir des codes de confirmation à usage unique dans l'application ou scannez le code QR depuis l'Assistant d'authentification de la Web Console.

   c. Saisissez le code de confirmation généré pour vous authentifier et vous connecter à la Web Console.

3. Test du Serveur d'administration

1. Vérifiez que l'interface de Web Console fonctionne correctement lorsque vous êtes connecté en tant que kscadmin ou en tant qu'autres utilisateurs.

2. Exécutez successivement les tâches suivantes :

   - Téléchargement des mises à jour dans le stockage du Serveur d'administration
   - Maintenance du Serveur d'administration
   - Sauvegarde des données du Serveur d'administration

   > Remplacez les chemins Windows dans les paramètres des tâches par des répertoires Linux sur le nouveau Serveur d'administration, ou supprimez les tâches et configurez-les à partir de zéro.

3. Vérifiez les résultats des tâches et, si nécessaire, modifiez les paramètres des tâches, les stratégies d'administration et les paramètres du Serveur d'administration.

4. Restauration de la connexion des appareils administrés au FQDN du Serveur d'administration précédent

Si vous avez attribué un nouveau FQDN au nouveau Serveur d'administration (par exemple, ksclinux.example.com), ajoutez l'un des types d'enregistrements DNS suivants :

- Un enregistrement CNAME faisant correspondre l'ancien nom du Serveur d'administration au nouveau nom du Serveur d'administration.

  Pour savoir comment configurer les enregistrements nécessaires, consultez la documentation de votre serveur DNS.

- Enregistrements A et AAAA pour l'adresse précédente du Serveur d'administration, qui pointe vers la nouvelle adresse IP du Serveur d'administration.

  Pour un service DNS basé sur Windows Server, exécutez les commandes avec les valeurs applicables à votre infrastructure.

Pour ajouter un enregistrement DNS de type A pour un service DNS basé sur Windows Server, exécutez les commandes avec les valeurs applicables à votre infrastructure.

1. Connectez-vous à votre serveur DNS.

2. Ouvrez PowerShell et obtenez l'adresse IP à partir de l'enregistrement A existant en exécutant la commande suivante :

   ```
   Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
   ```

3. Modifiez l'adresse IP dans l'enregistrement A en exécutant les commandes suivantes :

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Vérifiez que l'adresse IP dans l'enregistrement A a été mise à jour en exécutant la commande suivante :

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

Le résultat de la commande inclut l'adresse IP du Serveur d'administration de Kaspersky Security Center Linux. Les appareils administrés se reconnecteront après la mise à jour du cache DNS local.

6 Configuration de la protection antivirus du Serveur d'administration

Pour respecter les recommandations du Guide de renforcement de la sécurité en matière de protection antivirus du Serveur d'administration, installez les applications de Kaspersky sur le Serveur d'administration et configurez les stratégies d'administration. Pour déployer Kaspersky Endpoint Security for Linux, consultez le guide de déploiement.

L'installation et la configuration comprennent les étapes suivantes :

1. Création d'un groupe d'administration distinct

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Hiérarchie des groupes**.
2. Cochez la case en regard du groupe **Appareils administrés**.
3. Cliquez sur **Ajouter**.
4. Dans la fenêtre qui s'affiche, indiquez un nom pour le nouveau groupe (par exemple, *kscserver*) et confirmez sa création en cliquant sur le bouton **Ajouter**.

2. Création d'une stratégie pour l'Agent d'administration sans héritage des paramètres

1. Dans la fenêtre principale de Web Console, accédez à la section **Gestion des actifs** → **Stratégies**.
2. Cliquez sur le bouton **Ajouter**.
3. Dans l'Assistant de création de la stratégie, sélectionnez l'application **Agent d'administration de Kaspersky Security Center** et cliquez sur **Suivant**.
4. Désactivez l'option **Hériter des paramètres de la stratégie parente** et cliquez sur **Enregistrer**.

3. Installation du plug-in d'administration de Kaspersky Endpoint Security for Linux depuis Kaspersky Security Center ou manuellement

Vous pouvez installer le plug-in d'administration de Kaspersky Endpoint Security for Linux de l'une des manières suivantes :

- Installation depuis la liste des paquets de distribution disponibles dans Web Console.
- Installation manuelle à partir d'un fichier.

Pour installer le plug-in d'administration de Kaspersky Endpoint Security depuis la liste des paquets de distribution disponibles dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.

2. Cliquez sur le bouton **Ajouter**.

   La liste des plug-ins d'administration disponibles s'ouvre. La liste est mise à jour automatiquement lorsque de nouvelles versions de plug-ins Web sont publiées.

3. Dans la liste des plug-ins disponibles, sélectionnez la dernière version disponible du plug-in Internet pour Kaspersky Endpoint Security for Linux.

4. Dans la fenêtre qui s'ouvre avec une description du plug-in Web, cliquez sur le bouton **Installer le plug-in**.

5. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in s'affichera dans la liste des plug-ins Internet installés.

Vidéo : Installation du plug-in Internet d'administration à l'aide de l'Assistant



Pour installer manuellement le plug-in d'administration de Kaspersky Endpoint Security à partir d'un fichier :

1. Téléchargez l'archive contenant le plug-in Internet depuis la page de téléchargement des applications, dans la section Kaspersky Endpoint Security for Linux : **Plug-in de Contrôle des applications** → **Plug-in de la Web Console**.

2. Décompressez localement l'archive téléchargée.

3. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.

4. Cliquez sur le bouton **Ajouter à partir d'un fichier**.

5. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez le chemin d'accès au fichier plugin.zip et le chemin d'accès au fichier signature.txt.

   Les fichiers se trouvent dans le dossier dans lequel vous avez décompressé l'archive contenant le plug-in Internet.

6. Cliquez sur le bouton **Ajouter**.

7. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in s'affichera dans la liste des plug-ins Internet installés (**Paramètres** → **Plug-ins Web**).

Vidéo : Installation du plug-in Internet d'administration dans les réseaux isolés



4. Création d'une stratégie pour Kaspersky Endpoint Security for Linux sans héritage des paramètres

En cas d'utilisation de Kaspersky Endpoint Security for Linux avec Kaspersky Security Center Linux, vous devez gérer les paramètres de la stratégie conformément aux recommandations des experts de Kaspersky.

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Sélectionnez un groupe d'administration pour le Serveur d'administration.

3. Cliquez sur **Ajouter**.

   L'Assistant de création de la stratégie démarre.

4. Dans la fenêtre qui s'ouvre, sélectionnez Kaspersky Endpoint Security for Linux dans la liste.

5. Spécifiez **Mode standard ou mode Endpoint Detection and Response Agent** de l'application Kaspersky Endpoint Security for Linux.

6. Indiquez si vous avez l'intention de participer au Kaspersky Security Network.

7. Consultez les recommandations d'optimisation pour les appareils administrés.

8. Dans le nom de la stratégie, indiquez que la stratégie appartient au Serveur d'administration.
9. Désactivez l'option **Hériter des paramètres de la stratégie parent**.
10. Enregistrez vos modifications.

Vidéo : création d'une stratégie



5. Création de la tâche de groupe Update pour Kaspersky Endpoint Security for Linux

1. Dans la fenêtre principale de la Web Console, sélectionnez la section **Tâches**.
2. Sélectionnez un groupe d'administration pour le Serveur d'administration.
3. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.
4. Dans la fenêtre qui s'ouvre, sélectionnez Kaspersky Endpoint Security for Linux dans la liste.
5. Spécifiez le type de tâche *Update* et passez aux étapes suivantes sans modifier les paramètres.

   La fenêtre des propriétés de la tâche s'ouvre.
6. Dans la section **Paramètres de l'application → Sources des mises à jour**, activez la source Kaspersky Security Center et augmentez sa priorité.

Dans un réseau isolé, utilisez Kaspersky Update Utility pour créer un référentiel pour les tâches de mise à jour.

Vidéo : configuration des mises à jour centralisées des bases de données



6. Ajout d'une clé de licence au stockage du Serveur d'administration avec fonctionnalité de distribution automatique des clés

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, accédez à la section **Licences**.
2. Cliquez sur **Ajouter**.
3. Spécifiez l'option **Code d'activation** et cliquez sur **Envoyer**.

   Dans un réseau isolé, utilisez un fichier clé que vous pouvez demander à l'aide du service https://keyfile.kaspersky.com/fr-FR.
4. Dans la liste des licences, cliquez sur le nom de la licence.
5. Cochez la case **Distribuer automatiquement la clé de licence sur les appareils administrés**.
6. Enregistrez vos modifications.

Vidéo : activation de l'application à l'aide d'un code d'activation



Vidéo : activation de l'application à l'aide d'un fichier clé



7. Création de paquets d'installation pour l'Agent d'administration et Kaspersky Endpoint Security for Linux

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des logiciels → Paquets d'installation**.
2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation démarre.
3. Choisissez le **Générer un paquet d'installation pour une application Kaspersky**.
4. Dans la liste des applications, recherchez la dernière version de Kaspersky Endpoint Security for Linux et cliquez sur son nom.
5. Dans la barre latérale, lancez le téléchargement en cliquant sur le bouton **Télécharger et créer le paquet d'installation**.

   Lisez et acceptez les Contrats de licence utilisateur final pour commencer à utiliser les applications.
6. Revenez à la liste des applications et téléchargez la dernière version de l'Agent d'administration pour Linux.

   Lisez et acceptez les Contrats de licence utilisateur final pour commencer à utiliser les applications.
7. Dans la fenêtre principale de la Web Console, dans la liste des applications téléchargées, cliquez sur les noms des applications.

Dans un réseau isolé, téléchargez les paquets de distribution depuis le site de Kaspersky et sélectionnez l'option **Générer un paquet d'installation à partir d'un fichier** dans l'Assistant de création du paquet d'installation.

Vidéo : création automatique d'un paquet d'installation dans Kaspersky Security Center



Vidéo : création manuelle d'un paquet d'installation dans Kaspersky Security Center



8. Installation de l'Agent d'administration pour Linux

1. Dans la fenêtre principale de la Web Console, sélectionnez **Gestion des logiciels** → **Paquets d'installation**.
2. Cochez la case en regard du paquet **Agent d'administration Kaspersky pour Linux**.
3. Cliquez sur **Développer**.

   L'Assistant de déploiement de protection démarre.
4. Sélectionnez l'option **Utilisation d'un paquet autonome**.
5. À l'étape **Déplacer les appareils vers le dossier Appareils administrés**, ignorez la configuration des règles de déplacement des appareils vers un groupe d'administration. Cette option n'est pas applicable à l'appareil du Serveur d'administration.
6. À l'étape **Résultat de la création du paquet d'installation autonome**, sélectionnez et copiez le chemin d'accès complet vers le script d'installation de l'application.
7. Dans le système d'exploitation du Serveur d'administration, ouvrez la ligne de commande.

8. Lancez l'installation du paquet autonome :

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

où `</var/opt/.../stand-alone_package_sh>` est le chemin d'accès complet précédemment copié vers le fichier de script du paquet d'installation autonome de l'application.

Si l'installation réussit, une notification correspondante s'affiche.

9. Déplacez l'appareil du Serveur d'administration (par exemple, *ksclinux*) du groupe **Appareils administrés** vers un groupe d'administration préparé auparavant (par exemple, *kscserver*).

9. Installation de Kaspersky Endpoint Security for Linux

1. Dans la fenêtre principale de la Web Console, sélectionnez **Gestion des logiciels** → **Paquets d'installation**.
2. Cochez la case en regard du paquet Kaspersky Endpoint Security for Linux.
3. Cliquez sur **Développer**.

   L'Assistant de déploiement de protection démarre.
4. Sélectionnez l'option **Utilisation d'un paquet autonome**.
5. À l'étape **Résultat de la création du paquet d'installation autonome**, sélectionnez et copiez le chemin d'accès complet vers le script d'installation de l'application.
6. Dans le système d'exploitation du Serveur d'administration, ouvrez la ligne de commande.
7. Lancez l'installation du paquet autonome :

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

où `</var/opt/.../stand-alone_package_sh>` est le chemin d'accès complet précédemment copié vers le fichier de script du paquet d'installation autonome de l'application.

Si l'installation réussit, une notification correspondante s'affiche.

8. Dans la fenêtre principale de la Web Console, dans la section **Tâches**, sélectionnez le nœud racine dans la liste des groupes d'administration portant le nom du Serveur d'administration.
9. Dans la liste des tâches du Serveur d'administration, lancez les tâches suivantes dans l'ordre :
   - Téléchargement des mises à jour dans le stockage du Serveur d'administration
   - Update (Kaspersky Endpoint Security for Linux)
10. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Actifs (Appareils)**.
11. Cliquez sur le nom de l'objet Appareil du Serveur d'administration.
12. Vérifiez les principaux indicateurs de l'état de l'appareil :
    - Dernière mise à jour des bases antivirus (actuellement).
    - Connexion au Serveur d'administration (actuellement).

- État de la protection (en cours d'exécution).
- Événement *Clé ajoutée* (présent).

Utilisez le guide de déploiement de Kaspersky Endpoint Security for Linux pour déployer la solution de sécurité sur les appareils de votre réseau.

Mise à jour d'une ancienne version de l'application

L'application Kaspersky Endpoint Security peut être mise à jour en installant à distance ou localement une nouvelle version de l'application sur les appareils protégés.

Vous pouvez réaliser la mise à jour vers Kaspersky Endpoint Security 12.5 for Linux uniquement depuis Kaspersky Endpoint Security 12.4 for Linux.

Il n'est pas possible de mettre à jour Kaspersky Endpoint Security des versions antérieures vers la version 12.5. Si vous disposez d'une version antérieure de Kaspersky Endpoint Security, vous devez d'abord la désinstaller, puis installer Kaspersky Endpoint Security 12.5 for Linux.

Vous pouvez suivre ces étapes pour mettre l'application à niveau.

1 Préparation de l'environnement

Avant de lancer la mise à jour de Kaspersky Endpoint Security, effectuez les étapes préparatoires nécessaires en fonction de votre infrastructure.

2 Préparation des paquets de distribution

Sélectionnez un paquet de distribution en fonction de votre système d'exploitation, de son architecture et du type de processeur.

3 Mise à jour du plug-in d'administration de Kaspersky Endpoint Security

Si vous gérez l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, mettez à jour le plug-in Internet d'administration ou le plug-in MMC d'administration de Kaspersky Endpoint Security, selon la console que vous utilisez pour gérer Kaspersky Security Center.

4 Mise à jour de l'application et de l'interface graphique sur les appareils protégés

Installez la nouvelle version de l'application sur vos appareils protégés. Pour l'application mise à jour, le mode d'utilisation de l'application sélectionné lors de l'installation est conservé. Si vous souhaitez utiliser l'application dans un mode différent, vous devez désinstaller l'application, puis suivre la procédure d'installation et de configuration initiale de l'application.

Si vous utilisez Kaspersky Endpoint Security en mode standard ou en mode Agent EDR et que vous utilisez l'interface graphique de l'application, mettez également à jour l'interface graphique.

Vous pouvez mettre à jour l'application et l'interface graphique de l'application des manières suivantes :

- À distance, à l'aide de Kaspersky Security Center.
- Localement, via la ligne de commande ;

Comment mettre l'application à niveau à partir d'un paquet RPM à l'aide de la ligne de commande

La mise à jour de l'application via la ligne de commande revient à installer une nouvelle version de l'application sur l'appareil.

Vous devez disposer des privilèges root pour mettre l'application à jour.

Pour mettre l'application à niveau, exécutez la commande suivante :

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

L'application Kaspersky Endpoint Security redémarre automatiquement.

Symboles

Options de la commande

Paramètre	Description
`KESL_EULA_AGREED=yes`	Acceptez les conditions du Contrat de licence utilisateur final.
`KESL_PRIVACY_POLICY_AGREED=yes`	Acceptez les conditions de la Politique de confidentialité.
`KESL_USE_KSN=yes/no`	Utilisation de Kaspersky Security Network : `yes` : accepter les conditions de la Déclaration de Kaspersky Security Network et activer l'utilisation de Kaspersky Security Network. `no` : refuser les conditions de la Déclaration de Kaspersky Security Network et désactiver l'utilisation de Kaspersky Security Network.
`<arch>`	Type d'architecture : `i386` : pour les systèmes d'exploitation 32 bits `x86_64` : pour les systèmes d'exploitation 64 bits `aarch64` : pour les systèmes d'exploitation 64 bits pour l'architecture Arm

L'application Kaspersky Endpoint Security redémarre automatiquement.

Exemple :

```
Mettez à jour le paquet d'application RPM avec le paquet d'interface graphique pour les systèmes d'exploitation 64 bits :

# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Les modifications apportées aux paramètres de l'application après la fin de la mise à jour et avant le redémarrage de l'application ne sont pas enregistrées.

Comment mettre l'application à niveau à partir d'un paquet DEB à l'aide de la ligne de commande

La mise à jour de l'application via la ligne de commande revient à installer une nouvelle version de l'application sur l'appareil.

Vous devez disposer des privilèges root pour mettre l'application à jour.

Pour mettre l'application à niveau, exécutez la commande suivante :

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

L'application Kaspersky Endpoint Security redémarre automatiquement.

Symboles

Options de la commande

Paramètre	Description
`KESL_EULA_AGREED=yes`	Acceptez les conditions du Contrat de licence utilisateur final.
`KESL_PRIVACY_POLICY_AGREED=yes`	Acceptez les conditions de la Politique de confidentialité.
`KESL_USE_KSN=yes/no`	Utilisation de Kaspersky Security Network : `yes` : accepter les conditions de la Déclaration de Kaspersky Security Network et activer l'utilisation de Kaspersky Security Network. `no` : refuser les conditions de la Déclaration de Kaspersky Security Network et désactiver l'utilisation de Kaspersky Security Network.
`<arch>`	Type d'architecture : `i386` : pour les systèmes d'exploitation 32 bits `amd64` : pour les systèmes d'exploitation 64 bits `arm64` : pour les systèmes d'exploitation 64 bits pour l'architecture Arm

Exemple :

```
Mettez à jour le paquet d'application DEB avec le paquet d'interface graphique pour les systèmes d'exploitation 64 bits :

# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

Les modifications apportées aux paramètres de l'application après la fin de la mise à jour et avant le redémarrage de l'application ne sont pas enregistrées.

5 Mise à jour de l'Agent d'administration de Kaspersky Security Center

Étape facultative. Si vous gérez de manière centralisée Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, mettez à jour l'Agent d'administration sur les appareils protégés. La mise à jour s'effectue en installant une nouvelle version de l'Agent d'administration.

Sur un appareil exécutant le système d'exploitation Astra Linux Special Edition, il est recommandé de mettre à jour l'Agent d'administration à distance à l'aide de Kaspersky Security Center, car la mise à jour à l'aide de la ligne de commande dans la console d'administration de Kaspersky Security Center entraîne la création d'un nouvel exemplaire de cet appareil géré, et l'ancien n'est plus disponible. Pour plus de détails, consultez l'aide de Kaspersky Security Center.

Pendant la mise à jour de l'Agent d'administration, l'application continue de fonctionner correctement.

Particularités de la mise à jour à partir d'une version précédente de l'application

- En cas d'erreur lors de la mise à jour de l'application, la mise à jour est annulée et la version antérieure de l'application est lancée. Dans ce cas, un message d'erreur s'affiche, mais la nouvelle version (rpm/dkpg) apparaît dans le gestionnaire de paquets.

- Sur un système d'exploitation avec un gestionnaire de paquets de type `rpm`, si le paquet d'application et le paquet d'interface graphique sont tous deux installés, nous déconseillons de mettre à jour un seul des paquets sans l'autre.

  Sur un système d'exploitation avec un gestionnaire de paquets de type `dpkg`, si le paquet d'application et le paquet d'interface graphique sont tous deux installés, aucun des paquets ne peut être mis à jour sans l'autre.

- Si une nouvelle version de l'application modifie les termes du Contrat de licence et/ou de la Politique de confidentialité, vous devez accepter les nouveaux termes lors de la mise à jour de l'application. Les textes des contrats d'utilisation sont disponibles sur le site Internet de Kaspersky (dans la section **CLUF**), ainsi que dans le répertoire `~/.kesl/12.5/license.<language ID>`.

  Si vous n'acceptez pas les termes du Contrat de licence et/ou de la Politique de confidentialité, l'application ne sera pas mise à jour.

- Si les conditions de la déclaration de Kaspersky Security Network ont changé dans la nouvelle version de l'application, vous devez accepter ou refuser les nouvelles conditions d'utilisation de Kaspersky Security Network. Vous trouverez le texte de la Déclaration de Kaspersky Security Network dans ~/.kesl/12.5/ksn_license.<language ID>. Le refus d'utiliser Kaspersky Security Network n'interrompt pas le processus de mise à jour. Vous pouvez activer, désactiver ou modifier le mode de Kaspersky Security Network ultérieurement.

  Si vous avez utilisé KSN dans la version précédente de l'application et avez accepté les termes de la déclaration de Kaspersky Security Network, vous devez accepter les termes de la déclaration de Kaspersky Security Network lors de la mise à jour de la version de l'application. Dans le cas contraire, l'utilisation de KSN sera désactivée.

- Que l'application Kaspersky Endpoint Security ait été lancé avant le démarrage du processus de mise à jour ou non, si la mise à jour a réussi, une nouvelle version de l'application est lancée.

- Lorsque vous mettez à jour une version d'une application, les fichiers de vidage de la version précédente sont supprimés.

- Lors de la mise à jour de l'application, le fichier journal des événements de la version précédente devient le premier fichier des événements dans l'ensemble de fichiers de la version actuelle. Ce fichier sera stocké jusqu'à ce que le nombre d'événements dans les fichiers restants atteigne le nombre maximal spécifié (spécifié dans le paramètre `MaxEventsNumber`). Par conséquent, une situation temporaire peut survenir dans laquelle l'application stocke deux fois plus d'événements que spécifié dans le paramètre `MaxEventsNumber`.

- Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode Agent EDR, il est recommandé d'exécuter la tâche de mise à jour des bases de données après la mise à jour de l'application.

À propos de la mise à jour des plug-ins de gestion de Kaspersky Endpoint Security

La mise à jour du plug-in d'administration de Kaspersky Endpoint Security s'effectue en installant une nouvelle version du plug-in d'administration. En fonction de la Console d'administration de Kaspersky Security Center que vous utilisez, vous devrez installer :

- le plug-in Internet d'administration de Kaspersky Endpoint Security

- le plug-in MMC d'administration de Kaspersky Endpoint Security

Comment installer le plug-in Internet d'administration

Vous pouvez installer le plug-in Internet de l'une des manières suivantes :

- À l'aide de l'Assistant de configuration initiale de Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console vous invite automatiquement à exécuter l'assistant de configuration initiale lors de la première connexion de Kaspersky Security Center Web Console au Serveur d'administration. Vous pouvez également exécuter l'assistant de configuration initiale dans l'interface de Kaspersky Security Center Web Console (**Découverte et déploiement des appareils → Déploiement et attribution → Assistant de configuration initiale**). L'Assistant de configuration initiale de l'application peut également vérifier l'actualité des plug-ins Internet installés et charger les mises à jour indispensables. Pour en savoir plus sur l'Assistant de configuration initiale de Kaspersky Security Center Web Console, consultez l'aide de Kaspersky Security Center.

- Manuellement, à l'aide d'un paquet de distribution provenant de la liste des plug-ins Internet de Kaspersky ou d'un fichier.

Pour installer manuellement le plug-in Internet de Kaspersky Endpoint Security depuis Kaspersky Security Center :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Configuration → Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.

2. Cliquez sur le bouton **Ajouter**.

   La liste des plug-ins d'administration disponibles s'ouvre. La liste est mise à jour automatiquement lorsque de nouvelles versions de plug-ins Web sont publiées.

3. Dans la liste des plug-ins disponibles, sélectionnez le plug-in Internet de **Kaspersky Endpoint Security <numéro de version> for Linux**.

4. Dans la fenêtre qui s'ouvre avec une description du plug-in Web, cliquez sur le bouton **Installer le plug-in**.

5. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in s'affichera dans la liste des plug-ins Internet installés (**Configuration** → **Plug-ins Web**).

Pour installer manuellement le plug-in Internet de Kaspersky Endpoint Security à partir d'un fichier :

1. Téléchargez l'archive contenant le plug-in Internet depuis la page de téléchargement des applications, dans la section **Kaspersky Endpoint Security for Linux** (**Paquet de distribution complémentaire** → **Plug-in de la Web Console**).

2. Décompressez localement l'archive téléchargée.

3. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Paramètres** → **Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.

4. Cliquez sur le bouton **Ajouter à partir d'un fichier**.

5. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez le chemin d'accès au fichier plugin.zip et le chemin d'accès au fichier signature.txt. Les fichiers se trouvent dans le dossier dans lequel vous avez décompressé l'archive contenant le plug-in Internet.

6. Cliquez sur le bouton **Ajouter**.

7. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in apparaît dans la liste des plug-ins Web installés (**Paramètres** → **Plug-ins Web**).

Si, dans les propriétés du Serveur d'administration de Kaspersky Security Center, vous avez sélectionné une langue qui n'est pas incluse dans le kit de distribution de l'application Kaspersky Endpoint Security, le Contrat de licence utilisateur final et toute l'interface de Kaspersky Security Center Web Console seront affichés en anglais.

Comment installer le plug-in d'administration MMC

Avant d'installer le plug-in MMC d'administration de Kaspersky Endpoint Security, il faut s'assurer que Kaspersky Security Center et Redist C ++ 2015 (Microsoft Visual C ++ 2015 Redistributable) sont installés.

Pour installer le plug-in MMC :

1. Téléchargez le fichier klcfginst.msi depuis la page de téléchargement des applications, dans la section **Kaspersky Endpoint Security for Linux** (**Version** → **Plug-in d'administration**).

2. Sur l'appareil où est installée la Console d'administration de Kaspersky Security Center, exécutez le fichier klcfginst.msi.

Après l'installation, le plug-in MMC d'administration s'affiche dans la liste des plug-ins MMC d'administration installés dans les propriétés du Serveur d'administration de Kaspersky Security Center.

Pour afficher la liste des plug-ins MMC d'administration installés :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le **nœud Serveur d'administration <nom du serveur>** et ouvrez la fenêtre des propriétés du Serveur d'administration de l'une des manières suivantes :

   - Ouvrez le menu contextuel du nœud **Serveur d'administration <nom du serveur>** et sélectionnez l'élément **Propriétés**.

   - Cliquez sur le lien **Propriétés du Serveur d'administration** dans la zone de travail du nœud **Serveur d'administration <nom du serveur>** de la section **Serveur d'administration**.

2. Dans la liste de gauche, dans la section **Avancés**, sélectionnez la section **Informations sur les plug-ins d'administration installés des applications**.

   Dans la partie droite de la fenêtre, la liste des plug-ins d'administration installés affiche le plug-in MMC d'administration de Kaspersky Endpoint Security : **Kaspersky Endpoint Security <numéro de version> for Linux**.

Conversion des stratégies et des tâches

Les stratégies et les tâches configurées pour les versions précédentes de l'application Kaspersky Endpoint Security ne sont pas compatibles avec la version mise à jour de l'application. Si vous utilisez la Console d'administration de Kaspersky Security Center pour gérer l'application, après avoir mis à jour le plug-in MMC d'administration, vous pouvez convertir les stratégies et les tâches à l'aide de l'Assistant de conversion groupée des stratégies et des tâches de Kaspersky Security Center (pour plus de détails, consultez l'aide de Kaspersky Security Center).

Les stratégies et les tâches converties portent le nom « *<Nom de la stratégie ou de la tâche d'origine> (convertie)* ».

Dans les stratégies et tâches converties, la plupart des paramètres utilisent les valeurs configurées pour la version précédente de l'application. Certains paramètres ont des valeurs spéciales. Les paramètres qui manquaient dans les stratégies et les tâches de la version précédente prennent des valeurs par défaut dans les stratégies et les tâches converties.

Vous ne pouvez pas convertir les stratégies et les tâches dans Kaspersky Security Center Web Console.

Si vous utilisez Web Console pour gérer l'application, vous devez créer de nouvelles stratégies et tâches pour l'application dans Kaspersky Security Center. Vous pouvez transférer certaines valeurs des paramètres des stratégies et des tâches d'une version précédente d'une stratégie ou d'une tâche vers une nouvelle version en exportant et en important les paramètres.

Considérations particulières relatives aux plug-ins d'administration

- Les plug-ins d'administration de la version précédente continuent de fonctionner après l'installation d'une nouvelle version des plug-ins d'administration de Kaspersky Endpoint Security. Avec leur aide, vous pouvez gérer la version précédente de l'application Kaspersky Endpoint Security.

  Si vous avez mis à jour l'application sur tous les appareils clients, vous pouvez supprimer les plug-ins d'administration de Kaspersky Endpoint Security de la version précédente.

- Lors de l'installation d'une nouvelle version du plug-in MMC d'administration de la même version de l'application, vous devez d'abord supprimer le plug-in MMC déjà installé de cette version, puis installer le nouveau plug-in MMC de cette version.

Paramètres de l'application après la mise à jour

Si vous utilisez la Console d'administration de Kaspersky Security Center pour gérer l'application, vous pouvez *convertir les stratégies* afin que la nouvelle version utilise les valeurs des paramètres de stratégie spécifiées pour la version précédente de l'application (pour plus d'informations, consultez l'aide de Kaspersky Security Center).

Vous ne pouvez pas convertir les stratégies dans Kaspersky Security Center Web Console.

Lorsque vous mettez à jour une application à l'aide de la ligne de commande, la plupart des paramètres reprennent leurs valeurs de la version précédente de l'application. Vous pouvez également migrer les paramètres de l'application en exportant les paramètres vers un fichier et en les important à partir d'un fichier.

Les paramètres qui manquaient dans la version précédente de l'application prennent des valeurs par défaut. Certains paramètres ont des valeurs spéciales.

Paramètres d'interception des événements système

Si le mécanisme d'interception des événements système basé sur le module de noyau mis à jour était sélectionné dans la version précédente de l'application, après la mise à jour, l'application utilise la technologie fanotify pour intercepter les événements système. Ensuite, après la mise à jour des bases et des modules de l'application et un redémarrage automatique, l'application revient à l'utilisation du module de noyau mis à jour.

Paramètres de Kaspersky Security Network

Après la conversion d'une stratégie dans le plugin MMC, les paramètres d'utilisation de Kaspersky Security Network dans les propriétés de la stratégie dépendent de si vous avez accepté ou refusé les conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion des stratégies et des tâches :

- Si vous avez accepté les conditions de la Déclaration, l'option **Mode étendu de KSN** est sélectionnée.

- Si vous avez rejeté les conditions de la Déclaration, l'option **Ne pas utiliser KSN** est sélectionnée.

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `UseKSN` est modifié comme suit :

- Si vous définissez `KESL_USE_KSN=No` lors de la mise à niveau, `UseKSN=No`.
- Si vous définissez `KESL_USE_KSN=Yes` lors de la mise à niveau, `UseKSN=Extended`.
- Dans d'autres cas, la valeur du paramètre `UseKSN` ne change pas après la mise à jour.

Paramètres d'utilisation du mode cloud

Après la conversion d'une stratégie dans le plug-in MMC, les paramètres d'utilisation du mode cloud peuvent changer selon le fait que vous avez accepté ou refusé les conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion des stratégies et des tâches :

- Si vous avez accepté les conditions de la Déclaration, la case **Activer le mode cloud** sera cochée.
- Si vous refusez les conditions de la Déclaration, la case **Activer le mode cloud** sera décochée.

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `CloudMode` est défini sur les valeurs suivantes :

- `CloudMode=No`, si le paramètre `UseKSN=No` après la mise à jour ;
- `CloudMode=Yes` si `UseKSN=Basic/Extended` a été défini après la mise à jour et `CloudMode=Yes` a été défini avant la mise à jour.

Le mode Cloud est disponible si l'utilisation de KSN est activée. Pour activer le mode cloud, vous avez besoin de :

- dans la Console d'administration ou dans la Web Console, sélectionnez l'option **Mode étendu de KSN** et cochez la case **Activer le mode Cloud**.
- Sur la ligne de commande, définissez les paramètres suivants :

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

Paramètres d'intégration avec Kaspersky Managed Detection and Response

Si le module MDR a été activé, après la conversion de la stratégie dans le plug-in MMC, l'état du module MDR dépend de votre acceptation ou de votre rejet des conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion de stratégie et de tâche :

- Si vous avez accepté les conditions de la Déclaration, le module MDR restera activé (la case **Activer Managed Detection and Response** est cochée).
- Si vous avez rejeté les conditions de la Déclaration, la case **Activer Managed Detection and Response** sera décochée.

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `UseMDR` est défini sur les valeurs suivantes :

- `UseMDR=No`, si le paramètre `UseKSN=No` après la mise à jour ;
- `UseMDR=Yes` si `UseKSN=Basic/Extended` a été défini après la mise à jour et `UseMDR=Yes` a été défini avant la mise à jour.

Si vous souhaitez utiliser la fonctionnalité Kaspersky Managed Detection and Response, vous devez activer l'utilisation de Kaspersky Security Network en mode avancé.

Paramètres d'intégration avec Endpoint Detection and Response Expert

La nouvelle version de l'application propose un mode d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).

L'intégration de Kaspersky Endpoint Security for Linux à Kaspersky Endpoint Detection and Response Expert (cloud) est temporairement indisponible. Il est prévu que cette fonctionnalité soit prise en charge d'ici fin 2026. Consultez régulièrement nos notes de mise à jour pour vous tenir informé des mises à niveau des applications et des nouvelles fonctionnalités.

Après la conversion de la stratégie dans le plug-in MMC, l'intégration avec Endpoint Detection and Response Expert (cloud) est désactivée (la case **Activer Endpoint Detection and Response Expert (cloud)** est décochée). L'application utilise l'intégration avec Endpoint Detection and Response Expert (on-premises).

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `EDR_EXPERT_CLOUD_MODE` est défini sur : `EDR_EXPERT_CLOUD_MODE=No` (valeur par défaut).

Paramètres des autorisations utilisateur

La nouvelle version de l'application prend en charge la Protection par mot de passe.

Après la conversion de la stratégie dans le plug-in MMC, la protection par mot de passe est désactivée.

Après la mise à niveau de l'application à l'aide de la ligne de commande, les autorisations des utilisateurs sont conservées conformément aux rôles utilisateur (*kesladmin*, *kesluser*, *keslaudit*, *nokesl*) configurés dans la version précédente de l'application.

Suppression d'une application

Vous pouvez suivre ces étapes pour désinstaller Kaspersky Endpoint Security.

Considérations particulières relatives à la suppression de Kaspersky Endpoint Security for Linux

- Pendant le processus de désinstallation de l'application, toutes les tâches de Kaspersky Endpoint Security sur l'appareil seront arrêtées.
- Après la désinstallation de l'application, toutes les informations enregistrées par l'application sont supprimées, y compris les certificats d'application qui ont été installés. La base de données de licences est conservée et vous pouvez l'utiliser pour réinstaller l'application. L'identifiant unique de l'ordinateur (SensorID) est également enregistré.
- Si l'application a été installée sur un système systemd, une fois l'application désinstallée, les paramètres systemd reprennent leur valeur d'origine.

1 Suppression de l'application et de l'interface graphique de l'application

Désinstallez les paquets de l'application et les paquets de l'interface graphique des appareils protégés.

Vous pouvez supprimer le paquet de l'application et le paquet de l'interface graphique en même temps, ou vous pouvez désinstaller uniquement le paquet de l'interface graphique. Il est impossible de supprimer uniquement le paquet de l'application si le paquet de l'interface graphique est installé.

Vous pouvez supprimer l'application et l'interface graphique de l'application des manières suivantes :

À distance, à l'aide de Kaspersky Security Center.

Localement, via la ligne de commande ;

La désinstallation requiert les privilèges root.

Une fois la procédure de suppression terminée, un message sur les résultats de la suppression s'affiche.

Suppression du paquet de l'application et du paquet de l'interface utilisateur graphique

```
Désinstaller l'application et l'interface graphique installées à partir de paquets RPM
```

```
rpm -e kesl kesl-gui
```

```
Désinstaller l'application et l'interface utilisateur graphique installées à partir de paquets DEB
```

```
apt-get purge kesl kesl-gui
```

Suppression du paquet de l'application utilisé sans interface graphique

```
Supprimer l'application installée à partir d'un paquet RPM
```

```
rpm -e kesl
```

```
Supprimer l'application installée à partir d'un paquet DEB
```

```
apt-get purge kesl
```

Suppression du paquet de l'interface utilisateur graphique

Désinstaller l'interface graphique de l'application installée à l'aide d'un paquet au format RPM

```
rpm -e kesl-gui
```

Désinstaller l'interface graphique de l'application installée à l'aide d'un paquet au format DEB

```
apt-get purge kesl-gui
```

La suppression s'effectue en arrière-plan.

2 Suppression de l'Agent d'administration

Si vous avez utilisé Kaspersky Security Center pour gérer l'application Kaspersky Endpoint Security, vous devez supprimer l'Agent d'administration des appareils protégés.

Vous pouvez désinstaller l'Agent d'administration des manières suivantes :

À distance, à l'aide de Kaspersky Security Center.

Localement, via la ligne de commande ;

La désinstallation requiert les privilèges root.

Une fois la procédure de suppression terminée, un message sur les résultats de la suppression s'affiche.

Désinstaller l'Agent d'administration installé sur un système d'exploitation 32 bits à l'aide d'un paquet au format RPM

```
rpm -e klnagent
```

Désinstaller l'Agent d'administration installé sur un système d'exploitation 64 bits à l'aide d'un paquet au format RPM

```
rpm -e klnagent64
```

Désinstaller l'Agent d'administration installé sur un système d'exploitation 32 bits à l'aide d'un paquet au format DEB

```
apt-get purge klnagent
```

Désinstaller l'Agent d'administration installé sur un système d'exploitation 64 bits à l'aide d'un paquet au format DEB

```
apt-get purge klnagent64
```

3 Suppression du plug-in d'administration de Kaspersky Endpoint Security

Si vous avez utilisé Kaspersky Security Center pour gérer Kaspersky Endpoint Security, vous devez désinstaller le plug-in Internet d'administration ou le plug-in MMC d'administration de Kaspersky Endpoint Security, selon la console que vous avez utilisée pour gérer Kaspersky Security Center.

Comment supprimer le plug-in MMC d'administration de Kaspersky Endpoint Security

1. Fermez la Console d'administration de Kaspersky Security Center.
2. Sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée, ouvrez l'éditeur du registre Windows et accédez à :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   Cette branche contient des données sur tous les plug-ins d'administration installés dans la Console d'administration. Le nom de l'application gérée se trouve dans le paramètre **DisplayName**.
3. Sélectionnez la section qui correspond au plug-in de l'application Kaspersky Endpoint Security de la version requise.
4. Ouvrez le paramètre **UninstallString** et copiez sa valeur.
5. Ouvrez la ligne de commande avec les droits d'administrateur, collez la valeur copiée et appuyez sur la touche **Enter**.

Comment supprimer le plug-in Internet de Kaspersky Endpoint Security

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Configuration → Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.
2. Cochez la case **Kaspersky Endpoint Security <version number> for Linux**.
3. Cliquez sur **Supprimer**.

   Confirmez la désinstallation du plug-in Internet.

Utilisation de l'application

Par défaut, l'application Kaspersky Endpoint Security est lancée automatiquement au démarrage du système d'exploitation (pour les niveaux d'exécution par défaut applicables à chacun des systèmes d'exploitation).

Lorsque l'application est lancée avec la configuration par défaut, les modules suivants sont démarrés :

- Protection contre les fichiers malicieux.
- Contrôle des appareils.
- Détection comportementale.
- Protection contre les menaces Internet : uniquement si l'un des navigateurs pris en charge est installé dans le système d'exploitation et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas installé dans les propriétés de la stratégie).
- Protection contre les menaces réseau : uniquement si les paramètres de la protection contre les menaces réseau sur l'appareil sont définis via une stratégie. Par défaut, la protection contre les menaces réseau est activée dans les propriétés de la stratégie. Si votre appareil utilise des paramètres configurés localement, la protection contre les menaces réseau est désactivée par défaut.

Au démarrage de l'application, des tâches de service sont automatiquement lancées sur l'appareil afin d'assurer le fonctionnement de fonctions supplémentaires de l'application : la fonction d'activation de l'application et la fonction Sauvegarde.

Par défaut, l'application exécute également des tâches personnalisées configurées sur la ligne de commande et configurées pour s'exécuter après le démarrage de l'application (mode de lancement `PS`).

Si vous arrêtez l'application, toutes les tâches sur en cours d'exécution sur l'appareil sont interrompues. Les tâches définies par l'utilisateur interrompues en mode d'exécution PS ne reprennent pas là où elles ont été interrompues. Au prochain lancement de l'application, une telle tâche sera exécutée depuis le début au lieu de reprendre là où elle a été interrompue. Pour plus d'informations sur les types de tâches, consultez la section Tâches locales de Kaspersky Endpoint Security.

L'état de Kaspersky Endpoint Security est surveillé par le service watchdog. Ce service est lancé automatiquement au lancement de l'application. En cas de plantage de l'application, un fichier de vidage est produit et l'application se relance automatiquement.

Comment démarrer ou arrêter l'application à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste, sélectionnez l'appareil sur lequel vous souhaitez démarrer ou arrêter l'application, puis cliquez sur le lien portant le nom de l'appareil pour ouvrir la fenêtre des propriétés de ce dernier.

3. Choisissez l'onglet **Applications**.

4. Cochez la case en regard de l'application Kaspersky Endpoint Security.

5. Exécutez une des actions suivantes :

   - Si vous souhaitez exécuter l'application, cliquez sur le bouton **Démarrer**.
   - Si vous souhaitez arrêter l'application, cliquez sur le bouton **Arrêter**.

Vous pouvez surveiller l'état de fonctionnement de l'application à l'aide du widget **État de la protection** dans la fenêtre **Surveillance et rapports / Panneau de surveillance**.

Comment démarrer ou arrêter l'application à l'aide de la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil sur lequel vous voulez démarrer ou arrêter l'application. Dans le menu contextuel du appareil, sélectionnez **Propriétés**.
4. Dans la fenêtre **Propriétés : <Nom de l'appareil>**, choisissez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Choisissez l'application Kaspersky Endpoint Security.
6. Exécutez une des actions suivantes :

    – démarre l'application.

    – arrête l'application.

   Vous pouvez également gérer l'application à partir du menu contextuel.

Comment démarrer ou arrêter l'application à l'aide de la ligne de commande

Pour pouvoir lancer l'application, le compte utilisateur root doit être propriétaire des répertoires suivants, et seul le propriétaire doit y avoir un accès en écriture : /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Système d'exploitation avec systemd

```
Démarrer l'application
```

```
systemctl start kesl
```

```
Arrêter l'application
```

```
systemctl stop kesl
```

```
Redémarrer l'application
```

```
systemctl restart kesl
```

```
Afficher l'état actuel de l'application
```

```
systemctl status kesl
```

Système d'exploitation avec init

Démarrer l'application

```
service kesl start
```

Arrêter l'application

```
service kesl stop
```

Redémarrer l'application

```
service kesl restart
```

Afficher l'état actuel de l'application

```
service kesl status
```

Licence

Licence est un droit d'utilisation limité dans le temps de Kaspersky Endpoint Security, qui vous est accordé selon les termes du contrat de licence conclu (Contrat de licence). La liste des fonctions disponibles et la durée d'utilisation de l'application dépendent de la licence sous laquelle l'application est utilisée.

Types de licence

Gratuite

- *Évaluation* : une licence gratuite qui permet de découvrir les fonctionnalités de l'application.

  La licence d'évaluation a une courte durée. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, il faut acheter une licence commerciale.

  Vous ne pouvez activer l'application avec une licence d'essai qu'une seule fois. Une fois l'application activée avec une licence commerciale, elle ne peut plus être activée avec une licence d'évaluation.

- La *licence d'évaluation de Kaspersky Security Center Cloud Console* est une licence destinée à l'évaluation de Cloud Console. Avec cette licence, vous pouvez effectuer des actions dans un espace de travail pendant 30 jours. Tous les applications administrées, y compris l'application Kaspersky Endpoint Security, sont automatiquement activés sous la licence d'évaluation de Kaspersky Security Center Cloud Console. Vous ne pouvez pas activer l'application Kaspersky Endpoint Security avec votre propre licence d'évaluation après l'expiration de votre licence d'évaluation pour Cloud Console.

  L'espace de travail d'essai sera automatiquement supprimé avec tout son contenu à l'expiration de la période de 30 jours.

Payante

- *Commerciale* – licence payante fournie lors de l'achat de l'application.

  Après l'expiration de la licence commerciale, l'application cesse d'exercer ses fonctions principales. Pour continuer à utiliser Kaspersky Endpoint Security, vous devez renouveler la licence commerciale. Une fois votre licence expirée, vous ne pouvez plus utiliser l'application et devez la supprimer de votre appareil.

- Un *abonnement* est un bon de commande pour l'application avec des paramètres spécifiques (date de fin de la durée de validité de l'abonnement, nombre d'appareils protégés). Vous pouvez souscrire un abonnement auprès d'un prestataire de services de votre région.

  L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Si l'abonnement est limité, une période de grâce de renouvellement vous est proposée après sa date d'expiration. Pendant cette période, l'application continue à fonctionner. C'est le prestataire de services qui décide d'octroyer ou non une période de grâce et en cas d'octroi, il détermine la durée.

  Vous pouvez gérer votre abonnement, y compris le résilier, sur le site du prestataire de services.

Fonctionnement des licences

1. **Vous recevrez un code d'activation**

   Après avoir acheté une solution Kaspersky sur le site Internet officiel de Kaspersky ou auprès de l'un de nos partenaires, vous recevrez un message à l'adresse email que vous avez indiquée lors de l'achat. Ce message contiendra un code d'activation et des informations sur la manière d'obtenir un fichier clé. Vous pouvez avoir besoin d'un fichier clé si votre organisation ne prend pas en charge l'activation en ligne de l'application à l'aide d'un code.

   > Si vous avez souscrit un abonnement à Kaspersky Endpoint Security, le prestataire de services vous fournira uniquement un code d'activation.

2. **Activation de l'application**

   Ensuite, vous devez *activer l'application*, c'est-à-dire rendre une licence d'application valide. Pour ce faire, vous devez ajouter une clé de licence à l'application à l'aide de votre code d'activation ou de votre fichier clé.

   Les méthodes d'activation suivantes sont proposées :

   - À distance via Kaspersky Security Center
   - Dans la ligne de commande.
   - Via l'interface graphique

   Mode standard

   Pour utiliser l'application en mode standard, vous pouvez utiliser des licences qui couvrent différents périmètres de fonctionnalités. Si certains modules ne sont pas couverts par votre licence, il se peut que vous ayez besoin d'une autre clé de licence :

   - Clé de licence Kaspersky Endpoint Detection and Response Optimum Add-on (ci-après également dénommée *clé EDR Optimum*), pour activer le module Kaspersky EDR Optimum
   - Clé de licence Kaspersky Unified Monitoring and Analysis Platform Add-on (ci-après également dénommée *clé KUMA*), pour activer l'intégration avec la fonctionnalité Kaspersky Unified Monitoring and Analysis Platform
   - Clé de licence Kaspersky Managed Detection and Response Optimum/Expert Add-on (ci-après également dénommée *clé MDR*), pour activer le module Kaspersky MDR
   - Clé de licence Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on (ci-après également dénommée *clé EDR Expert (on-premises)*), pour activer le module EDR Expert (on-premises)

- Clé de licence Kaspersky Endpoint Detection and Response Expert (cloud) Add-on (ci-après également dénommée *clé EDR Expert (cloud)*), pour activer le module EDR Expert (cloud)

- Clé de licence Kaspersky Workload Security Module Add-on (ci-après également dénommée *clé KWSM*), pour activer les modules Contrôle de l'intégrité du système et Analyse du conteneur

Si ces modules ne sont pas couverts par votre licence, vous ne pouvez les activer qu'après avoir activé l'application Kaspersky Endpoint Security elle-même.

Mode EDR Agent

Si vous utilisez l'application Kaspersky Endpoint Security en mode EDR Agent, vous avez besoin d'une clé de licence EDR Expert (on-premises) pour l'activer.

Mode Light Agent

Si vous utilisez Kaspersky Endpoint Security en mode Light Agent, vous n'avez pas besoin d'ajouter une clé à l'application. Vous activez Kaspersky Security for Virtualization Light Agent côté Serveur de protection.

Le module Endpoint Detection and Response Optimum et les modules d'intégration aux solutions Kaspersky sont également activés côté Serveur de protection.

Résolution des problèmes d'activation de l'application

3. **Renouvellement d'une licence ou d'un abonnement**

Nous vous recommandons de surveiller votre licence ou votre abonnement afin de procéder à son renouvellement en temps opportun. Nous vous recommandons de renouveler la licence avant sa date d'expiration afin de garantir la protection continue de votre appareil contre les menaces de sécurité.

Pour renouveler la licence en temps opportun, vous pouvez utiliser une clé de réserve. Vous pouvez renouveler votre abonnement manuellement ou automatiquement sur le site de votre prestataire de services. L'abonnement illimité se renouvelle automatiquement si le montant dû au prestataire de services est versé dans les délais.

Particularités de l'ajout de clés

- Une clé de licence d'évaluation ou une clé d'abonnement ne peut pas être ajoutée en tant que clé de réserve.

- La date d'expiration de la clé de réserve doit être ultérieure à celle de la clé active.

- Si une clé active ainsi qu'une clé de réserve ont été ajoutées à l'application et que vous ajoutez une nouvelle clé active, la nouvelle clé remplace la clé active précédemment ajoutée ; si vous ajoutez une nouvelle clé de réserve, elle remplace la clé de réserve précédemment ajoutée.

- Si une clé active et des clés permettant d'activer le module Endpoint Detection and Response Optimum et les modules d'intégration aux solutions Kaspersky ont été ajoutées à l'application, et que vous avez ajouté une seule clé de réserve pour une licence couvrant également le module Endpoint Detection and Response Optimum et les modules d'intégration, alors, après l'expiration de la clé active, la clé de réserve devient active et libère les autres clés actives. Vous pouvez ensuite utiliser ces clés pour activer le module Endpoint Detection and Response Optimum et les modules d'intégration sur un autre appareil.

4. **Affichage des informations sur les clés de licence ajoutées**

Vous pouvez consulter les informations sur les clés de licence ajoutées à l'application à distance à l'aide de Kaspersky Security Center, ou localement sur un appareil protégé à l'aide de la ligne de commande ou de l'interface graphique.

Articles utiles

Contrat de licence utilisateur final

Le *Contrat de licence utilisateur final* est un accord juridique conclu entre vous et AO Kaspersky Lab qui prévoit les conditions d'utilisation de l'application que vous avez achetée.

Veuillez lire attentivement les termes du Contrat de licence avant d'utiliser l'application.

Vous pouvez prendre connaissance du Contrat de licence utilisateur final et de la Politique de confidentialité, qui décrit le traitement et la mise à disposition des données :

- Avant d'installer l'application, dans le fichier license.<identifiant de langue>. Ce fichier est fourni dans le kit de distribution de l'application.
- Pendant l'installation de l'application Kaspersky Endpoint Security.

  En confirmant votre acceptation des conditions du Contrat de licence utilisateur final et de la Politique de confidentialité lors de la création du paquet d'installation de l'application (si elle est installée à l'aide de Kaspersky Security Center) ou lors de la configuration initiale de l'application (si l'installation est effectuée à l'aide de la ligne de commande), vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous n'acceptez pas les termes du Contrat de licence et de la Politique de confidentialité, vous devez mettre fin à l'installation de l'application et ne devez pas utiliser l'application.

- Après l'installation de l'application, les fichiers contenant les textes du Contrat de licence utilisateur final de l'application Kaspersky et de la Politique de confidentialité se trouvent sur l'appareil protégé dans le répertoire /opt/kaspersky/kesl/doc/license.<identifiant de langue>.

Code d'activation

Un *code d'activation* est une séquence unique de 20 caractères alphanumériques.

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

Si le code d'activation a été perdu après l'activation du programme, contactez le partenaire de Kaspersky auprès duquel vous avez acheté la licence.

Fichier clé

Un *fichier clé* est un fichier portant l'extension key que Kaspersky vous fournit. Pour activer l'application à l'aide d'un fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky.

Si un fichier clé a été supprimé par accident, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer votre fichier clé, effectuez l'une des actions suivantes :

- Contacter le vendeur de la licence.
- Obtenez un fichier clé sur le site Internet de Kaspersky à partir de votre code d'activation existant.

Clé de licence

La *clé de licence* est une séquence de bits qui vous permet d'activer, puis d'utiliser l'application conformément aux dispositions du Contrat de licence. La clé de licence est créée par les spécialistes de Kaspersky.

La clé avec laquelle l'application est actuellement activée devient la *clé de licence active*. En tant que clé active, vous pouvez ajouter une clé de licence d'évaluation, une clé de licence commerciale (clé commerciale) ou une clé d'abonnement.

Clé de réserve

Une *clé de licence de réserve* est une clé de licence qui permet à l'utilisateur d'utiliser l'application mais qui n'est pas actuellement en cours d'utilisation. La clé de licence de réserve s'active automatiquement lorsque la période de validité de la licence associée à la clé de licence active expire. Une clé de réserve ne peut être ajoutée qu'après l'ajout d'une clé active.

Une clé de licence d'évaluation peut être ajoutée en tant que clé de licence active. Une clé de licence pour une licence d'évaluation ne peut pas être ajoutée en tant que clé de licence de réserve.

Comment passer à une autre solution Kaspersky

Si l'application est utilisée en mode Light Agent, les clés de licence sont administrées dans la solution Kaspersky Security for Virtualization Light Agent.

Suivez ces étapes si votre organisation a déployé une solution Kaspersky, si Kaspersky Endpoint Security est utilisé en mode standard ou en mode Agent EDR, et si vous devez passer à une autre solution Kaspersky.

1. **Préparer une nouvelle licence**

   Achetez une autre solution Kaspersky sur le site Internet de Kaspersky ou auprès de nos partenaires. Vous recevrez un message à l'adresse email que vous avez indiquée lors de l'achat. Ce message contiendra un code d'activation et des informations sur la manière d'obtenir un fichier clé.

   Si vous avez précédemment activé l'application Kaspersky Endpoint Security à l'aide d'un code d'activation, vous devrez également utiliser un code d'activation cette fois-ci. Si vous avez précédemment activé l'application à l'aide d'un fichier clé, vous devrez utiliser un fichier clé.

2. **Remplacer votre licence**

   Vous pouvez remplacer une licence des manières suivantes :

   - À distance, à l'aide de Kaspersky Security Center. Ajoutez la clé de licence au Stockage du Serveur d'administration et distribuez-la aux appareils protégés.
   - À partir de la ligne de commande à l'aide de la commande suivante : `kesl-control [-L] --add-active-key <path to key file / activation code>`.
   - Dans l'interface graphique, supprimez la clé actuellement appliquée à l'application et ajoutez la nouvelle clé.

3. **Vérifier que la licence a bien été remplacée**

   Pour ce faire, consultez les détails de la clé de licence utilisée sur vos appareils protégés.

Articles utiles

Code d'activation

Un *code d'activation* est une séquence unique de 20 caractères alphanumériques.

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

Si le code d'activation a été perdu après l'activation du programme, contactez le partenaire de Kaspersky auprès duquel vous avez acheté la licence.

Fichier clé

Un *fichier clé* est un fichier portant l'extension key que Kaspersky vous fournit. Pour activer l'application à l'aide d'un fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky.

Si un fichier clé a été supprimé par accident, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer votre fichier clé, effectuez l'une des actions suivantes :

- Contacter le vendeur de la licence.
- Obtenez un fichier clé sur le site Internet de Kaspersky à partir de votre code d'activation existant.

Gestion des clés de licence

Si l'application est utilisée en mode Light Agent, les clés de licence sont administrées dans la solution Kaspersky Security for Virtualization Light Agent. Les commandes de gestion des clés de licence échouent.

Gestion des clés à l'aide de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez ajouter des clés aux appareils administrés de différentes manières :

- À l'aide de la tâche *Ajouter une clé*. Cette méthode permet d'ajouter des clés à l'application sur un appareil individuel ou sur tous les appareils inclus dans un groupe d'administration. Lors de la création d'une tâche, la clé ajoutée au stockage des clés de Kaspersky Security Center est utilisée. Vous pouvez ajouter une clé de licence au stockage des clés au préalable ou lors de la création de la tâche Ajouter une clé.

- En distribuant aux appareils une clé stockée sur le Serveur d'administration de Kaspersky Security Center. Cette méthode permet d'ajouter automatiquement des clés aux appareils administrés déjà connectés à Kaspersky Security Center et aux nouveaux appareils administrés. Pour utiliser cette méthode, vous devez d'abord ajouter la clé au stockage des clés de Kaspersky Security Center.

  Lors de la distribution automatique d'une clé en tant que clé active ou de réserve, la restriction de licence sur le nombre d'appareil (définie dans les propriétés de la clé) est prise en compte. Une fois la restriction de licence atteinte, la distribution de cette clé aux appareils cesse automatiquement. Vous pouvez afficher le nombre d'appareils auxquels la clé a été ajoutée ainsi que d'autres données dans les propriétés de la clé sous l'onglet **Appareils**.

Comment ajouter une clé au stockage des clés de Kaspersky Security Center à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Licences Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, sélectionnez la méthode d'ajout de la clé au stockage :
   - **Saisissez un code d'activation** si vous souhaitez ajouter une clé à l'aide d'un code d'activation.
   - **Ajouter un fichier clé** si vous souhaitez ajouter une clé à l'aide d'un fichier clé.
4. Selon le mode d'ajout de la clé que vous avez sélectionné à l'étape précédente, effectuez l'une des actions ci-dessous :
   - Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.
   - Cliquez sur le bouton **Sélectionner le fichier de clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension .key.
5. Cliquez sur le bouton **Fermer**.

La clé ajoutée apparaîtra dans la liste de clés.

Comment ajouter une clé à l'application via Web Console à l'aide de la tâche Ajouter une clé

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

    a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

    b. Dans la liste déroulante **Type de tâche**, sélectionnez **Ajout d'une clé**.

    c. Dans le champ **Nom de la tâche**, saisissez une brève description, telle que *Activation de Kaspersky Endpoint Security*.

    d. Dans la section **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

    La fenêtre **Sélection de la licence** s'ouvre.

5. Si vous aviez préalablement ajouté la clé dans le stockage des clés de Kaspersky Security Center, choisissez dans la liste la clé et cliquez sur le bouton **Suivant**.

6. Si la clé dont vous avez besoin ne se trouve pas dans le stockage des clés, cliquez sur le lien **ajouter une nouvelle clé de licence**.

    a. Dans la fenêtre qui s'ouvre, sélectionnez la méthode d'ajout de la clé au stockage :

    - **Saisissez un code d'activation** si vous souhaitez ajouter une clé à l'aide d'un code d'activation.
    - **Ajouter un fichier clé** si vous souhaitez ajouter une clé à l'aide d'un fichier clé.

    b. Selon le mode d'ajout de la clé que vous avez sélectionné à l'étape précédente, effectuez l'une des actions ci-dessous :

    - Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.
    - Cliquez sur le bouton **Sélectionner le fichier de clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension .key.

    c. Lisez les informations relatives à la clé et cliquez sur le bouton **Fermer**.

    d. La clé ajoutée apparaîtra dans la liste de clés. Sélectionnez-la dans la liste, puis cliquez sur le bouton **Suivant**.

7. Lisez les informations sur la licence et cliquez sur le bouton **Suivant**.

8. Dans l'onglet **Paramètres de l'application**, vous pouvez cocher la case **Utiliser comme clé de réserve**. Une clé ajoutée en tant que clé de réserve devient active après l'expiration de la clé actuelle.

9. Quittez l'Assistant.

    La nouvelle tâche apparaît dans la liste des tâches.

10. Cochez la case en regard de la tâche. Cliquez sur le bouton **Exécuter**.

Comment ajouter une clé à l'application à l'aide de Web Console en distribuant la clé aux appareils

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Licences Kaspersky**.
2. Ouvrez les propriétés de la clé en cliquant sur le lien portant le nom de l'application que la clé est censée activer.
3. Dans l'onglet **Général**, cochez la case **Distribuer automatiquement la clé de licence aux appareils administrés**.
4. Cliquez sur le bouton **Enregistrer**.

La clé de licence est alors distribuée automatiquement aux appareils clients appropriés.

Une nouvelle clé de licence ne sera ajoutée à l'appareil que si l'application sur cet appareil n'est pas encore activée ou si la licence expire dans moins de 14 jours.

Gestion des clés en ligne de commande

Pour gérer les clés de licence sur un appareil, vous pouvez utiliser les commandes de gestion des clés de licence.

Comment ajouter une clé à l'application

Vous pouvez utiliser ces commandes pour ajouter des clés afin d'activer l'application ou des modules qui ne sont pas couverts par votre licence. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

```
Ajouter une clé de licence active à l'application
```

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

Où :

- `path to key file` est le chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.
- `activation code` est le code d'activation.

```
Ajouter une clé de licence de réserve à l'application
```

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

Si la clé active n'a pas encore été ajoutée à l'application sur l'appareil, la commande échoue.

Comment supprimer une clé

Différentes commandes sont disponibles pour supprimer des clés.

```
Supprimer la clé active
```

```
kesl-control [-L] --remove-active-key
```

Supprimer la clé de réserve

```
kesl-control [-L] --remove-reserve-key
```

Supprimer la clé EDR Optimum active

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Supprimer la clé EDR Optimum de réserve

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Supprimer la clé KUMA active

```
kesl-control [-L] --remove-active-key --kuma
```

Supprimer la clé KUMA de réserve

```
kesl-control [-L] --remove-reserve-key --kuma
```

Supprimer la clé MDR active

```
kesl-control [-L] --remove-active-key --mdr
```

Supprimer la clé MDR de réserve

```
kesl-control [-L] --remove-reserve-key --mdr
```

Supprimer la clé de licence EDR Expert (on-premises) active

```
kesl-control [-L] --remove-active-key --edr-kata
```

Supprimer la clé de licence EDR Expert (on-premises) de réserve

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Supprimer la clé EDR Expert (cloud) active

```
kesl-control [-L] --remove-active-key --cxdr
```

Supprimer la clé EDR Expert (cloud) de réserve

```
kesl-control [-L] --remove-reserve-key --cxdr
```

Supprimer la clé KWSM active

```
kesl-control [-L] --remove-active-key --khcs
```

Supprimer la clé KWSM de réserve

```
kesl-control [-L] --remove-reserve-key --khcs
```

Gestion des clés dans l'interface graphique

Comment ajouter une clé de licence active

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira.

   En cliquant sur le bouton **Acheter une licence** dans cette fenêtre, vous pouvez ouvrir la boutique en ligne de Kaspersky, où vous pouvez acheter une licence.
3. Si vous souhaitez activer l'application sous licence commerciale :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Clé commerciale** et effectuez les actions suivantes en fonction de la méthode d'ajout de la clé :

      - Si vous souhaitez ajouter une clé à l'aide d'un code d'activation, saisissez le code d'activation et cliquez sur le bouton **Suivant**.
      - Si vous souhaitez ajouter une clé à l'aide d'un fichier de clé, ouvrez la fenêtre de sélection de fichier à l'aide du lien **Sélectionner un fichier clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension key.

      Cette fenêtre affiche les informations sur la clé et la licence qui lui est associée.

   b. Cliquez sur le bouton **Activer**.
4. Si vous souhaitez activer l'application à l'aide d'une licence d'évaluation, cliquez sur le bouton **Activer** dans le groupe **Clé d'évaluation**. Cette fenêtre affiche les informations sur la licence d'évaluation et la clé qui lui est associée.

Comment ajouter une clé de licence de réserve

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira. La fenêtre affiche des informations sur les clés de licence précédemment ajoutées.

3. Cliquez sur le bouton **Ajouter** et effectuez les actions suivantes en fonction de la méthode d'ajout de la clé :

   - Si vous souhaitez ajouter une clé à l'aide d'un code d'activation, saisissez le code d'activation et cliquez sur le bouton **Suivant**.

   - Si vous souhaitez ajouter une clé à l'aide d'un fichier de clé, ouvrez la fenêtre de sélection de fichier à l'aide du lien **Sélectionner un fichier clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension key.

   Cette fenêtre affiche les informations sur la clé et la licence qui lui est associée.

4. Cliquez sur le bouton **Ajouter**.

Comment supprimer une clé de licence

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.

   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira. La fenêtre affiche des informations sur les clés de licence précédemment ajoutées.

3. Cliquez sur le bouton **Supprimer** situé à droite des informations sur la clé que vous souhaitez supprimer.

4. Confirmez la suppression dans la fenêtre qui s'ouvre.

Articles utiles

Résolution des problèmes d'activation de l'application

Affichage des informations sur les clés de licence

Informations sur les clés de licence dans Kaspersky Security Center

Vous pouvez afficher des informations sur les clés de licence utilisées par Kaspersky Endpoint Security des manières suivantes :

- Dans les propriétés de la tâche *Ajouter une clé* que vous utilisez pour activer l'application, vous pouvez trouver des informations sur la clé que cette tâche ajoute à l'application.

- Dans les propriétés de l'application Kaspersky installée sur l'appareil client, vous pouvez trouver des informations sur les clés actives et les clés de réserve ajoutées à l'application sur cet appareil.

Comment afficher les informations sur les clés de licence d'un appareil via Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. La fenêtre des propriétés de l'application s'ouvre ; dans cette fenêtre, accédez à la section **Licences** sous l'onglet **Général**.

   La section affiche des informations sur les clés de licence ajoutées à l'application et les licences associées à ces clés :

   - **État de la clé de licence** désigne le type de la clé : active ou de réserve.
   - **Nom de l'application** : nom de la licence associée à la clé et les informations sur cette licence.
   - **Clé de licence** : clé de licence, une séquence alphanumérique unique.
   - **Type de licence** : type de licence : essai, commerciale ou abonnement.
   - **Date d'activation** : date à laquelle cette clé a été ajoutée.
   - **Date d'expiration** : date d'expiration de l'application activée à l'aide de cette clé.

Comment afficher les informations sur les clés de licence d'un appareil via la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.

5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.

6. Dans la fenêtre qui s'ouvre, accédez à la section **Clés de licence**.

La section affiche des informations sur les clés de licence actives et de réserve :

- **Numéro de série** : succession unique de caractères alphanumériques.
- **État** : état de la clé de licence, par exemple, actif ou de réserve.
- **Type** : le type de licence, commerciale ou évaluation.
- **Période de validité de la licence** : nombre de jours pendant lesquels il est possible d'utiliser l'application qui a été activée à l'aide de l'ajout de cette clé.
- **Limite** : nombre d'ordinateurs sur lesquels vous pouvez utiliser la clé.
- **Date d'activation** (le champ est disponible uniquement pour la clé active) : la date d'ajout de la clé active.
- **Date d'expiration** (le champ est accessible seulement pour la clé active) : la date d'expiration de la durée d'utilisation de l'application activée via l'ajout d'une clé active.

- Le rapport sur l'utilisation des clés de licence affiche des informations sur toutes les clés ajoutées via Kaspersky Security Center. Vous pouvez afficher le rapport d'utilisation des clés de licence à l'aide de Web Console (**Surveillance et rapports → Rapports**), ainsi qu'à l'aide de la Console d'administration (onglet **Rapports**). Pour afficher le rapport, vous devez sélectionner le modèle « Rapport d'utilisation de la clé de licence » dans la liste des rapports et commencer à générer le rapport.

- Le stockage des clés de licence de Kaspersky Security Center affiche des informations sur toutes les clés ajoutées au Serveur d'administration de Kaspersky Security Center. Vous pouvez ouvrir le stockage des clés à l'aide de Web Console (**Opérations → Licences de Kaspersky**), ainsi qu'à l'aide de la Console d'administration (dossier **Licences de Kaspersky**).

Vous pouvez également recevoir des informations sur les clés de licence utilisées et les licences qui leur sont associées à l'aide des notifications d'événements de Kaspersky Security Center. L'application envoie des informations sur l'expiration de la licence et la violation des restrictions de licence au Serveur d'administration de Kaspersky Security Center.

Informations sur les clés de licence sur l'appareil protégé

Comment afficher les informations sur les clés de licence dans la ligne de commande

```
Affichage des informations sur les clés de licence et les licences sur un appareil

kesl-control -L --query [--json]
```

où `--json` signifie que les données sont affichées au format JSON. Si vous ne spécifiez pas la clé `--json`, les paramètres seront affichés dans la console.

La commande affiche les informations suivantes sur la console :

- Informations sur la clé de licence active :
  - Date et heure de fin de la durée de validité de la licence.
  - Le nombre de jours avant l'expiration de la durée de validité de la licence.

    - Informations sur la limitation de la fonctionnalité de protection (cette ligne s'affiche uniquement pour la clé avec laquelle l'application Kaspersky Endpoint Security est activée).
    - Informations sur les limitations de mise à jour des bases de données de l'application.
    - Informations sur l'état de la clé de licence.
    - Le type de licence associé à la clé.
    - Limitation de la clé de licence (nombre d'unités de licence).
    - Le nom de l'application que la clé est censée activer.
    - Clé de licence active (séquence alphanumérique unique).
    - Date d'activation.
- Informations sur la clé de licence de réserve. S'affiche si l'application est utilisée en mode standard ou en mode EDR Agent et si une clé de réserve a été ajoutée. Si l'application est utilisée en mode Light Agent, les informations sur la clé de réserve ne sont pas affichées.
    - Date et heure de fin de la durée de validité de la licence.
    - Informations sur la limitation de la fonctionnalité de protection (cette ligne s'affiche uniquement pour une clé avec laquelle l'application Kaspersky Endpoint Security peut être activée).
    - Informations sur les limitations de mise à jour des bases de données de l'application.
    - Informations sur l'état de la clé de licence.
    - Le type de licence associé à la clé.
    - Limitation de la clé de licence (nombre d'unités de licence).
    - Le nom de l'application que la clé est censée activer.
    - Clé de licence de réserve (séquence alphanumérique unique).
    - La date et l'heure d'expiration de la licence associée à la clé active.

Vous pouvez également obtenir des informations sur la licence sous laquelle l'application est utilisée lors de l'affichage des détails de l'application :

```
kesl-control --app-info
```

Comment consulter les informations sur la licence et la clé dans l'interface graphique de l'application

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira.

   La fenêtre affiche des informations sur les clés actives et de réserve ajoutées à l'application. Cliquez sur le lien **En savoir plus** pour afficher des informations complètes sur les licences et les clés.

Le groupe **Licences actuelles** affiche les informations sur les clés actives ajoutées et les licences associées :

- Type de licence, restriction de licence et période de validité de la licence.
- **Clé de licence** : séquence alphanumérique unique.
- **État de la clé** : état de la clé ou message relatif à un problème de clé quelconque (le cas échéant).
- **Valide à partir du** : date d'activation de l'application via l'ajout de cette clé.
- **Expire** : nombre de jours avant la date de fin de validité de la licence et date de fin de validité de la licence (UTC).
- **Nom** : nom de l'application que la clé est destinée à activer.
- **Protection** : informations sur les restrictions sur les fonctions de protection et la fonction de mise à jour des bases de données d'application.

Le groupe **Clés de réserve** affiche les informations sur les clés de réserve ajoutées et les licences associées :

- Le type de clé de réserve, la restriction de licence et la période de validité de la licence associée à la clé.
- **Clé de licence** : séquence alphanumérique unique.
- **Type de licence** : type de licence associé à la clé de réserve.
- **Nom** : nom de l'application que la clé est destinée à activer.
- **Protection** : informations sur les restrictions sur les fonctions de protection et la fonction de mise à jour des bases de données d'application.

Si vous utilisez l'application Kaspersky Endpoint Security en mode standard ou en mode EDR Agent et utilisez Kaspersky Security Center pour gérer l'application, les informations sur l'ajout et la suppression de clés de licence et sur l'expiration de la durée de validité de la licence sont enregistrées par défaut dans le journal du système d'exploitation.

Interfaces d'administration de l'application

Pour gérer l'application Kaspersky Endpoint Security, vous pouvez utiliser :

- Kaspersky Security Center
- ligne de commande ;
- l'interface graphique de l'application a été améliorée.

  Vous ne pouvez effectuer qu'un sous-ensemble limité d'actions à l'aide de l'interface graphique de Kaspersky Endpoint Security.

Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour la protection des environnements virtuels, il n'est pas possible d'administrer l'application à l'aide de Kaspersky Security Center Cloud Console et de l'interface graphique de l'application.

Si l'application est utilisée en mode EDR Agent, seul un sous-ensemble limité des modules et des tâches de l'application est disponible. Vous pouvez gérer certains modules de protection, activer l'application et mettre à jour les bases de données. Pour en savoir plus sur les particularités du mode EDR Agent, consultez l'article Problèmes connus et limitations.

Choisissez un outil d'administration en fonction de l'infrastructure informatique de votre organisation, ainsi que du rôle et du processus de travail de l'administrateur. Nous vous recommandons d'administrer l'application sur les appareils clients à distance et de manière centralisée à l'aide de Kaspersky Security Center.

Administration de l'application via Kaspersky Security Center

Kaspersky Security Center vous permet de gérer à distance et de manière centralisée le fonctionnement de l'application Kaspersky Endpoint Security sur les appareils clients. Vous pouvez installer et désinstaller, démarrer et arrêter à distance l'application Kaspersky Endpoint Security ; configurer les paramètres de fonctionnement de l'application, des modules individuels et des tâches de l'application ; démarrer et arrêter des tâches sur les appareils gérés.

Groupes d'administration de Kaspersky Security Center

Pour utiliser Kaspersky Security Center afin d'administrer Kaspersky Endpoint Security installé sur des appareils, vous devez ajouter ces appareils aux *groupes d'administration*. Vous pouvez créer des groupes d'administration dans Kaspersky Security Center avant de commencer à installer Kaspersky Endpoint Security et configurer des règles visant à déplacer automatiquement les appareils vers les groupes d'administration. Vous pouvez également déplacer manuellement les appareils vers les groupes d'administration après avoir installé l'application (pour plus de détails, consultez l'Aide de Kaspersky Security Center).

Consoles d'administration et plug-ins d'administration

Pour gérer l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez utiliser les Consoles d'administration de Kaspersky Security Center suivantes :

- Console d'administration de Kaspersky Security Center (ci-après également, « Console d'administration »). Il s'agit d'un module logiciel enfichable pour Microsoft Management Console (MMC), qui est installé sur le poste de travail de l'administrateur et fournit une interface utilisateur aux services d'administration du Serveur d'administration et de l'Agent d'administration.

  L'interface de gestion de Kaspersky Endpoint Security via la Console d'administration de Kaspersky Security Center est fournie par le plug-in MMC d'administration de Kaspersky Endpoint Security (ci-après également, « plug-in MMC »).

  Le plug-in MMC doit être installé sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

- Kaspersky Security Center Web Console (ci-après également appelée *Web Console*). Il s'agit d'une interface Web permettant de gérer un système de protection basé sur les applications de Kaspersky. Vous pouvez travailler dans Kaspersky Security Center Web Console à l'aide d'un navigateur sur n'importe quel appareil.

  L'interface de gestion de Kaspersky Endpoint Security via Kaspersky Security Center Web Console est fournie par le plug-in Internet d'administration de Kaspersky Endpoint Security (ci-après également simplement « plug-in Internet »).

  Le plug-in Internet doit être installé sur l'appareil sur lequel Kaspersky Security Center Web Console est installée.

- Kaspersky Security Center Cloud Console. Il s'agit d'une Console d'administration cloud faisant partie de la version cloud de l'application Kaspersky Security Center, également appelée Kaspersky Security Center Cloud Console. La console cloud présente une interface similaire à celle de Kaspersky Security Center Web Console. L'interface de gestion de l'application Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console est également assurée par un plug-in Internet.

  Il n'est pas possible d'administrer l'application à l'aide de Kaspersky Security Center Cloud Console si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Kaspersky Endpoint Security fait partie de la solution Kaspersky Next Pro View. Pour plus d'informations sur les fonctionnalités de l'application disponibles dans cette solution, veuillez consulter l'aide de Kaspersky Next.

Stratégies et tâches de Kaspersky Security Center

Le plug-in MMC et le plug-in Web vous permettent de créer des stratégies et des tâches dans Kaspersky Security Center pour gérer le fonctionnement de l'application Kaspersky Endpoint Security :

- Une *stratégie* est un ensemble de paramètres appliqués à tous les appareils du groupe d'administration. À l'aide de stratégies, vous pouvez définir les mêmes valeurs des paramètres de l'application pour tous les appareils clients faisant partie du groupe d'administration.

  La stratégie de Kaspersky Endpoint Security définit les paramètres généraux de fonctionnement de l'application Kaspersky Endpoint Security et les paramètres de fonctionnement des modules fonctionnels individuels de l'application sur les appareils sur lesquels la stratégie est appliquée.

- Les *tâches* de Kaspersky Endpoint Security créées dans Kaspersky Security Center sont exécutées sur les appareils protégés et mettent en œuvre les fonctions de Kaspersky Endpoint Security telles que l'analyse à la demande, l'activation des applications, la mise à jour des bases de données et des modules de l'application.

  Dans Kaspersky Security Center, vous pouvez créer des tâches à exécuter sur un appareil individuel (tâches locales), ainsi que des tâches pour tous les appareils d'un groupe d'administration (tâches de groupe) ou des tâches pour une sélection aléatoire d'appareils (tâches pour des ensembles d'appareils).

À propos des politiques de Kaspersky Security Center

Une *stratégie* est un ensemble de paramètres de l'application Kaspersky Endpoint Security appliqués à tous les appareils clients faisant partie du groupe d'administration. La stratégie possède l'un des états suivants :

État de la stratégie

État	Description
Actif	La stratégie actuelle appliquée à l'appareil.
Inactive	Une stratégie qui n'est pas actuellement appliquée à l'appareil.
Pour les utilisateurs itinérants	Si cette option est sélectionnée, la stratégie entre en vigueur lorsque l'appareil quitte le réseau de l'entreprise.

Les stratégies suivent les règles suivantes :

- Vous pouvez configurer plusieurs stratégies avec des paramètres différents pour une même application.
- Une seule stratégie peut être active par application.
- Une stratégie peut avoir des stratégies enfants.

Verrouillage des paramètres

Chaque paramètre de stratégie possède l'attribut « cadenas ». L'état de cet attribut détermine si le paramètre sera transmis aux appareils administrés du groupe d'administration.

- Si le « cadenas » est fermé (🔒), cela signifie que le paramètre est appliqué aux appareils auxquels la stratégie s'applique. L'utilisateur ne peut pas modifier ces paramètres dans l'interface utilisateur de l'application administrée. On parle alors de paramètres *verrouillés*.
- Si le « cadenas » est ouvert (🔓), cela signifie que le paramètre n'est pas spécifié dans la stratégie. L'utilisateur peut modifier ces paramètres dans l'interface utilisateur de l'application administrée. On parle alors de paramètres *déverrouillés*.

Nous vous recommandons de verrouiller les paramètres de stratégie que vous souhaitez appliquer aux appareils administrés. Les paramètres de stratégie déverrouillés peuvent être remplacés sur un appareil administré.

Le nombre de paramètres avec un « cadenas » dans la Web Console et dans la Console d'administration peut varier.

Profil de stratégie

Pour éviter d'avoir à gérer un grand nombre de stratégies, par exemple lorsque seuls quelques paramètres doivent pouvoir être modifiés, vous pouvez utiliser des profils de stratégie.

Un *profil de stratégie* est un ensemble de paramètres de stratégie individuels qui diffèrent des paramètres de la stratégie « de base » et s'appliquent aux appareils clients lorsque les conditions configurées (règles d'activation) sont remplies. L'utilisation des profils de stratégie permet une configuration plus souple des paramètres de fonctionnement de l'application sur différents appareils.

Les paramètres du profil verrouillés remplacent les paramètres de la stratégie. Autrement dit, si le paramètre du profil verrouillé est différent du paramètre de la stratégie, l'application appliquera le paramètre du profil. Dans ce cas, les paramètres présentés sous forme de listes sont regroupés et se complètent. Autrement dit, si les paramètres de la liste de profils ne sont pas présents dans la stratégie « de base », ils compléteront la liste de paramètres résultante.

Les profils de stratégie suivent les règles suivantes :

- Un profil de stratégie prend effet lorsqu'une certaine condition d'activation est remplie.
- Les profils de stratégie contiennent des valeurs de paramètres différentes des valeurs définies dans la stratégie.
- L'activation d'un profil de stratégie modifie les paramètres effectifs de l'appareil administré (paramètres actuellement appliqués à l'appareil).
- Une stratégie peut avoir jusqu'à 100 profils.

Héritage des paramètres

Les stratégies, comme les groupes d'administration, présentent une hiérarchie. *Stratégie enfant* : il s'agit d'une stratégie de niveau hiérarchique imbriquée, c'est-à-dire une stratégie pour des groupes d'administration imbriqués et des Serveurs d'administration secondaires.

Par défaut, une stratégie enfant hérite des paramètres de la stratégie parent. Si un paramètre de la stratégie parent est verrouillé (), les stratégies enfants et les paramètres locaux de l'application reçoivent la même valeur, et le paramètre est verrouillé. Si nécessaire, vous pouvez désactiver l'héritage des paramètres de la stratégie parent. Les stratégies pour les utilisateurs autonomes ne fonctionnent pas selon la hiérarchie des groupes d'administration sur d'autres stratégies.

Si les paramètres de la stratégie enfant sont verrouillés (erreur *Accès refusé*), vérifiez les droits d'accès de l'utilisateur. Si l'utilisateur a le droit de modifier les paramètres de la stratégie, lancez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* pour Kaspersky Security Center et répétez l'autorisation. Cette erreur peut se produire après la mise à jour des plug-ins d'administration dans Kaspersky Security Center : après le téléchargement des mises à jour, l'application récupère les fichiers nécessaires pour la nouvelle version du plug-in d'administration.

Pour certains paramètres qui ont des listes comme valeurs (par exemple, des listes de règles ou des listes d'exclusions), vous pouvez activer la fusion des éléments de liste. Pour fusionner des éléments de la liste, vous devez procéder comme suit :

- Dans les propriétés de la stratégie enfant, sous l'onglet **Général**, activez le paramètre **Hériter des paramètres de la stratégie parent**.
- Dans les propriétés de la stratégie parent, fermer la liste avec un « cadenas » ().
- Dans les propriétés de la stratégie parent, activer la fusion des paramètres en cochant la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents de Kaspersky Security Center sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités.

Vous ne pouvez pas supprimer ou modifier les éléments de liste hérités dans une stratégie enfant. Les éléments de la liste fusionnés par héritage ne peuvent être supprimés ou modifiés que dans la stratégie parent. L'ajout, la modification et la suppression des éléments de la liste sont possibles à des niveaux inférieurs. De cette façon, vous pouvez configurer une liste dans une stratégie parent qui s'appliquera à toutes les stratégies enfants, et vous pouvez également ajouter des éléments à la liste dans la stratégie enfant.

Si vous supprimez un élément d'une liste fusionnée par héritage dans une stratégie parent, cet élément n'est pas supprimé des stratégies enfants. Pour supprimer cet élément des stratégies enfants, vous devez ouvrir les propriétés de ces stratégies et supprimer l'élément manuellement.

Certaines listes ne sont pas fusionnées. Dans ce cas, les paramètres du profil prévalent sur les paramètres de la stratégie « de base » :

- excluions dans les modules Protection contre les fichiers malicieux et Détection comportementale
- l'exclusion s'applique au fonctionnement des modules Protection contre les fichiers malicieux et Protection contre le chiffrement

- zones de surveillance dans le module Contrôle de l'intégrité du système
- liste des règles (dans la fenêtre **Règles du Contrôle des applications**) dans le module Contrôle des applications
- liste des règles dans le Contrôle Internet
- exclusions de la mémoire de processus de l'analyse des paramètres de l'application
- domaines de confiance dans les paramètres réseau
- certificats racines de confiance dans les paramètres réseau
- ports surveillés dans les paramètres réseau
- liste des adresses SVM dans les paramètres de découverte SVM

Les paramètres de fonctionnement de l'application changent conformément aux paramètres de la stratégie après la première application de la stratégie.

> Les paramètres d'une stratégie précédemment supprimée continuent de s'appliquer à l'appareil jusqu'à ce que celui-ci reçoive une nouvelle stratégie ou que ses paramètres soient modifiés localement.

Pour plus d'informations sur les stratégies et les profils de stratégie, ainsi que sur le mécanisme d'héritage des paramètres, consultez l'aide de Kaspersky Security Center.

Gestion des stratégies

Comment créer une stratégie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

   Une liste de stratégies et de profils de stratégie s'ouvre.

2. Sélectionnez le groupe d'administration auquel vous souhaitez appliquer la stratégie. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

3. Cliquez sur **Ajouter**.

   L'Assistant de création de la stratégie démarre.

4. Dans la fenêtre qui s'ouvre, sélectionnez le nom de l'application Kaspersky Endpoint Security dans la liste.

   Passez à l'étape suivante de l'Assistant.

5. Précisez dans quel mode vous utilisez l'application Kaspersky Endpoint Security :

- Dans **Mode standard ou mode Endpoint Detection and Response Agent**, l'application est utilisée pour protéger les appareils Linux en tant qu'application autonome ou en tant qu'application assurant la collaboration des solutions Detection and Response de Kaspersky et des solutions antivirus de fournisseurs tiers.

  Pour sélectionner ce mode, passez à l'étape suivante de l'Assistant.

- **Light Agent pour protéger les environnements virtuels** : dans le cadre de la solution Kaspersky Security for Virtualization Light Agent, l'application est utilisée pour protéger les machines virtuelles exécutant des systèmes d'exploitation invités Linux.

6. Si vous utilisez l'application en mode Light Agent, configurez les paramètres de détection des SVM :

   a. Sélectionnez la méthode utilisée par les Light Agents pour détecter les SVM disponibles pour la connexion :

   - **Utiliser le Serveur d'intégration**. Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant.

   - **Utiliser la liste d'adresses des SVM définie manuellement**. Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

   Si vous sélectionnez l'option **Utiliser la liste d'adresses des SVM définie manuellement**, que le Light Agent utilise l'algorithme avancé de sélection de la SVM et que le mode de protection des grandes infrastructures est activé sur une SVM, la connexion d'un Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez définir le paramètre **Emplacement des SVM** sur **Ignorer**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

   b. Si vous avez sélectionné le Serveur d'intégration, la fenêtre de l'Assistant affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. Si nécessaire, spécifiez de nouveaux paramètres de connexion :

      a. Cliquez sur le bouton **Configurer** et spécifiez les nouveaux paramètres de connexion dans la fenêtre qui s'ouvre :

      - **Adresse**. L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.

      - **Port**. Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

      Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

      b. Cliquez sur **Vérifier**.

c. Le plug-in Web vérifie le certificat SSL reçu du Serveur d'intégration. Si le certificat contient une erreur ou n'est pas approuvé, un message à ce sujet s'affiche dans la fenêtre **Paramètres de connexion au Serveur d'intégration**.

Vous pouvez visualiser les informations sur le certificat reçu du Serveur d'intégration en cliquant sur la ligne **Afficher le certificat reçu**.

> Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

Pour enregistrer le certificat reçu et continuer la connexion au Serveur d'intégration, dans le groupe **Sélection de l'action**, sélectionnez l'option **Ignorer**.

d. Spécifiez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **Vérifier**.

L'Assistant de création de la stratégie se connecte au Serveur d'intégration. Si la connexion échoue, un message d'erreur apparaît dans la fenêtre. Si la connexion est établie, la fenêtre **Connexion au serveur d'intégration** se ferme et l'état **Installé** s'affiche dans le champ **Connexion au serveur d'intégration** de la fenêtre de l'Assistant de création d'une stratégie.

c. Si vous sélectionnez une liste d'adresses SVM définie manuellement, créez une liste de SVM auxquelles les Light Agents administrés par cette stratégie peuvent se connecter. Pour ajouter une SVM à la liste, cliquez sur le bouton **Ajouter** et précisez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM dans la fenêtre qui s'ouvre. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

> Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application.

Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**.

Passez à l'étape suivante de l'Assistant.

7. Indiquez si vous avez l'intention d'utiliser Kaspersky Security Network. Pour ce faire, lisez attentivement la Déclaration de Kaspersky Security Network, puis effectuez l'une des opérations suivantes :

- Si vous acceptez toutes les conditions de la Déclaration et souhaitez utiliser Kaspersky Security Network avec l'application, sélectionnez **J'accepte les termes de Kaspersky Security Network**.
- Si vous ne souhaitez pas utiliser Kaspersky Security Network, sélectionnez **Je refuse les termes de Kaspersky Security Network** et confirmez votre décision dans la fenêtre qui s'ouvre.

Le refus d'utiliser Kaspersky Security Network n'entraîne pas l'arrêt de la création de la stratégie. Vous pouvez à tout moment activer ou désactiver l'utilisation de Kaspersky Security Network ou modifier le mode Kaspersky Security Network pour les appareils administrés dans les paramètres de la stratégie.

Passez à l'étape suivante de l'Assistant.

8. Vous serez invité à prendre connaissance des recommandations relatives à la configuration de Kaspersky Endpoint Security. Vérifiez les paramètres qui permettent à l'application d'optimiser l'utilisation des ressources système.

Passez à l'étape suivante de l'Assistant.

9. La fenêtre des paramètres de la nouvelle stratégie s'ouvre à l'onglet **Général**. Donnez un nom à la nouvelle stratégie.

   Vous pouvez également configurer les paramètres de stratégie suivants :

   - L'état de la stratégie.

     - **Active**. La stratégie est actuellement appliquée à l'appareil. Si cette option est sélectionnée, lors de la prochaine synchronisation de l'appareil avec le Serveur d'administration, cette stratégie deviendra active sur l'appareil. Cette option est sélectionnée par défaut.

     - **Inactive**. Si cette option est sélectionnée, la stratégie ne s'applique pas à l'appareil mais reste dans le dossier **Stratégies**. Vous pouvez activer une stratégie inactive.

     - **Pour les utilisateurs itinérants**. Si cette option est sélectionnée, la stratégie entre en vigueur lorsque l'appareil quitte le réseau de l'entreprise.

       > Dans la stratégie de l'Agent d'administration actuellement active sur l'appareil, dans la section **Réseau → Profils de connexion**, le paramètre **Activer le mode hors-ligne lorsque le Serveur d'administration est indisponible** doit être activé.

   - Héritage des paramètres de la stratégie :

     - **Hériter des paramètres de la stratégie parent**. Si le commutateur est activé, les valeurs des paramètres de la stratégie sont héritées de la stratégie de groupe de niveau supérieur. Les paramètres verrouillées ( ) dans la stratégie parent, ne sont pas accessibles à la modification. Le commutateur est activé par défaut.

     - **Forcer l'héritage des paramètres dans les stratégies enfants**. Si le commutateur est activé, les valeurs des paramètres de la stratégie seront propagés aux stratégies enfants. Dans les propriétés de la stratégie enfant, le commutateur **Hériter des paramètres de la stratégie parent** est automatiquement activé et ne peut pas être désactivé. Les paramètres de la stratégie enfant sont hérités de la stratégie parent, sauf les paramètres pour lesquels le "cadenas" ( ) est ouvert. Le bouton bascule est désactivé par défaut.

   Pour des informations générales sur les paramètres de stratégie, consultez l'aide de Kaspersky Security Center.

10. Si vous souhaitez gérer d'autres paramètres de stratégie, accédez à l'onglet **Paramètres de l'application** et apportez les modifications nécessaires.

    Vous pouvez également modifier les paramètres de la stratégie ultérieurement.

11. Cliquez sur le bouton **Enregistrer**.

Comment créer une stratégie dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant les appareils sur lesquels la stratégie doit être appliquée.

   Dans l'onglet **Appareils** du dossier portant le nom du groupe d'administration, vous pouvez consulter la liste des appareils faisant partie de ce groupe d'administration.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Cliquez sur le bouton **Nouvelle stratégie** pour lancer l'Assistant de création de stratégie.

   Vous pouvez également lancer l'Assistant à l'aide de l'élément **Créer → Stratégie** du menu contextuel de la liste des stratégies.

4. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security dans la liste.

   Passez à l'étape suivante de l'Assistant.

5. Saisissez le nom de la nouvelle stratégie.

6. Si vous souhaitez transférer les paramètres de la stratégie d'une version antérieure de Kaspersky Endpoint Security dans la stratégie en cours de création, cochez la case **Utiliser les paramètres de la stratégie de la version antérieure de l'application**.

   Passez à l'étape suivante de l'Assistant.

7. Indiquez si vous avez l'intention d'utiliser Kaspersky Security Network. Pour ce faire, lisez attentivement la Déclaration de Kaspersky Security Network, puis effectuez l'une des opérations suivantes :

   - Si vous acceptez l'intégralité des dispositions de la Déclaration et que vous souhaitez consulter le Kaspersky Security Network dans le cadre de l'utilisation de l'application, sélectionnez l'option **Je confirme avoir entièrement lu et compris les conditions de la Déclaration de Kaspersky Security Network, et je l'accepte**.

   - Si vous ne souhaitez pas utiliser Kaspersky Security Network, sélectionnez l'option **Je refuse d'utiliser Kaspersky Security Network** et confirmez votre choix dans la fenêtre qui s'ouvre.

   Le refus d'utiliser Kaspersky Security Network n'entraîne pas l'arrêt de la création de la stratégie. Vous pouvez à tout moment activer ou désactiver l'utilisation de Kaspersky Security Network ou modifier le mode Kaspersky Security Network pour les appareils administrés dans les paramètres de la stratégie.

   Passez à l'étape suivante de l'Assistant.

8. Précisez dans quel mode vous utilisez l'application Kaspersky Endpoint Security :

   - **Mode standard ou mode Endpoint Detection and Response Agent** : l'application est utilisée pour protéger les appareils fonctionnant sous systèmes d'exploitation Linux en tant qu'application autonome ou en tant qu'application assurant la collaboration des solutions Detection and Response de Kaspersky et des solutions antivirus de fournisseurs tiers.

   - **Mode Light Agent pour la protection des environnements virtuels** : l'application est utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent pour la protection des machines virtuelles exécutant des systèmes d'exploitation invités Linux.

   Passez à l'étape suivante de l'Assistant.

9. Si vous utilisez l'application en mode Light Agent, configurez les paramètres de détection des SVM :

   a. Sélectionnez la méthode utilisée par les Light Agents pour détecter les SVM disponibles pour la connexion :

      - **Utiliser le Serveur d'intégration**. Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant.

      - **Utiliser la liste d'adresses des SVM définie manuellement**. Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

Si vous sélectionnez l'option **Utiliser la liste d'adresses des SVM définie manuellement**, que le Light Agent utilise l'algorithme avancé de sélection de la SVM et que le mode de protection des grandes infrastructures est activé sur une SVM, la connexion d'un Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez définir le paramètre **Emplacement des SVM** sur **Ignorer**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

b. Si vous avez sélectionné le Serveur d'intégration, la fenêtre de l'Assistant affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. Si nécessaire, spécifiez de nouveaux paramètres de connexion :

   a. Cliquez sur le bouton **Modifier** et spécifiez les nouveaux paramètres de connexion dans la fenêtre qui s'ouvre :

      - **Adresse**. L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.

      - **Port**. Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

      Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

   b. Cliquez sur le bouton **OK**.

   c. Si l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée ne fait pas partie d'un domaine ou si votre compte n'est pas membre du groupe KLAdmins local ou du domaine ou du groupe des administrateurs locaux, le compte administrateur du Serveur d'intégration est utilisé pour l'authentification sur le Serveur d'intégration.

      Dans la fenêtre qui s'ouvre, saisissez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **OK**.

   d. Le plug-in MMC vérifie le certificat SSL reçu du Serveur d'intégration. Si le certificat contient une erreur ou n'est pas fiable, la fenêtre **Vérification du certificat du Serveur d'intégration** s'ouvrira. À l'aide du lien dans la fenêtre, vous pouvez afficher des informations sur le certificat reçu.

      Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

      Pour continuer à vous connecter au Serveur d'intégration, cliquez sur le bouton **Ignorer**. Le certificat reçu sera installé en tant que certificat de confiance sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

c. Si vous sélectionnez une liste d'adresses SVM définie manuellement, créez une liste de SVM auxquelles les Light Agents administrés par cette stratégie peuvent se connecter. Pour ajouter une SVM à la liste, cliquez sur le bouton **Ajouter** et précisez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM dans la fenêtre qui s'ouvre. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application.

Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**.

Passez à l'étape suivante de l'Assistant.

10. Le cas échéant, configurez les paramètres généraux de la Protection contre les fichiers malicieux.

    Passez à l'étape suivante de l'Assistant.

11. Si nécessaire, modifiez les paramètres par défaut de la protection contre les fichiers malveillants.

    Passez à l'étape suivante de l'Assistant.

12. Le cas échéant, configurez les exclusions de la Protection contre les fichiers malicieux.

    Passez à l'étape suivante de l'Assistant.

13. Si nécessaire, modifiez les actions par défaut lorsqu'une menace est détectée.

    Passez à l'étape suivante de l'Assistant.

14. Sélectionnez l'état de la stratégie :

    - **Stratégie active**. La stratégie est actuellement appliquée à l'appareil. Si cette option est sélectionnée, lors de la prochaine synchronisation de l'appareil avec le Serveur d'administration, cette stratégie deviendra active sur l'appareil. Cette option est sélectionnée par défaut.
    - **Stratégie inactive**. Si cette option est sélectionnée, la stratégie ne s'applique pas à l'appareil mais reste dans le dossier **Stratégies**. Vous pouvez activer une stratégie inactive.
    - **Stratégie pour les utilisateurs autonomes**. Si cette option est sélectionnée, la stratégie entre en vigueur lorsque l'appareil quitte le réseau de l'entreprise.

    Dans la stratégie de l'Agent d'administration actuellement active sur l'appareil, dans la section **Réseau → Profils de connexion**, le paramètre **Activer le mode hors-ligne lorsque le Serveur d'administration est indisponible** doit être activé.

15. Quittez l'Assistant de création de stratégie.

    La stratégie créée apparaîtra dans la liste des stratégies du groupe d'administration sous l'onglet **Stratégies** et dans le dossier **Stratégies** de l'arborescence de la console.

Pour des informations générales sur l'administration des stratégies, consultez l'aide de Kaspersky Security Center.

Articles utiles

Que faire si les tâches ne s'exécutent pas ou si les stratégies ne sont pas appliquées

Que faire si l'appareil affiche l'état : « Paramètres de stratégie non valides. La stratégie n'a pas été appliquée. »

Erreur : « L'application n'est pas prise en charge par la version actuelle de Kaspersky Security Center Web Console ou le plug-in Internet de l'application n'est pas installé »

Exportation et importation des paramètres d'une stratégie

Kaspersky Endpoint Security permet d'exporter une stratégie avec ses paramètres et ses profils dans un fichier KLP. Vous pouvez ensuite utiliser la fonctionnalité d'exportation/d'importation des stratégies pour sauvegarder des stratégies, les transférer vers un autre serveur ou, par exemple, les transférer de Kaspersky Security Center Windows vers Kaspersky Security Center Linux. Pour en savoir plus sur la gestion des stratégies, consultez l'aide de Kaspersky Security Center.

Comment exporter et importer une stratégie dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Stratégies**.
4. Pour exporter une stratégie, procédez comme suit :
   a. Cliquez sur la stratégie que vous souhaitez exporter.
   b. Cliquez sur le lien **Exporter la stratégie dans le fichier** situé dans la partie droite de la fenêtre.
   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format KLP dans lequel vous voulez exporter la stratégie et choisissez le dossier dans lequel vous souhaitez enregistrer le fichier.
   d. Enregistrez le fichier.
5. Pour importer une stratégie, procédez comme suit :
   a. Cliquez sur **Importer une stratégie à partir d'un fichier**.
   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de stratégie KLP que vous souhaitez importer.
   c. Ouvrez le fichier.

   Cette action ajoute une nouvelle stratégie avec l'état *Stratégie inactive*.

Comment exporter et importer la stratégie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Pour exporter une stratégie, procédez comme suit :
   a. Cochez la case en regard de la stratégie que vous souhaitez exporter.
   b. Appuyez sur le bouton **Exporter**.

c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format KLP dans lequel vous voulez exporter la stratégie et choisissez le dossier dans lequel vous souhaitez enregistrer le fichier.

d. Enregistrez le fichier.

3. Pour importer une stratégie, procédez comme suit :

a. Cliquez sur **Importer**.

b. Sélectionnez le fichier de stratégie KLP que vous souhaitez importer.

c. Une fois que la stratégie a été traitée, sélectionnez le groupe d'administration auquel vous souhaitez l'appliquer.

d. Cliquez sur le bouton **Terminée** pour terminer l'importation de la stratégie.

Cette action ajoute une nouvelle stratégie avec l'état *Inactive*.

Exportation et importation de certains paramètres d'une stratégie dans Web Console

Dans Web Console, vous pouvez exporter des paramètres individuels de stratégie vers un fichier JSON et importer de tels paramètres depuis un fichier. Par exemple, vous pouvez exporter une liste de règles du Contrôle Internet ou de zones de protection de la Protection contre les fichiers malicieux.

Les paramètres suivants sont disponibles pour l'exportation et l'importation :

- Zones de protection de la Protection contre les fichiers malicieux
- Filtres des pièces jointes de la Protection contre les menaces par emails
- Règles de paquet réseau
- Règles du Contrôle Internet
- Règles du Contrôle des applications
- Zones de contrôle et zones d'exclusion du Contrôle de l'intégrité du système
- Paramètres de la télémétrie
- Certaines exclusions de la Zone de confiance

Pour exporter ou importer des paramètres dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à la section à partir de laquelle vous souhaitez exporter ou importer des paramètres.

5. Appuyez sur le bouton .

6. Sélectionnez une action : **Importer** ou **Exporter**.

7. Si vous importez des paramètres, sélectionnez le fichier à partir duquel vous souhaitez importer les paramètres.

À propos des tâches de Kaspersky Endpoint Security créées dans Kaspersky Security Center

Vous pouvez créer les types de tâches suivants pour l'application Kaspersky Endpoint Security dans Kaspersky Security Center :

- tâches locales à exécuter sur des appareils individuels
- tâches de groupe à exécuter sur les appareils inclus dans le groupe d'administration
- Tâches pour une sélection d'appareils à exécuter sur plusieurs appareils, quelle que soit leur appartenance à des groupes d'administration.

Vous pouvez créer autant de tâches que nécessaire.

Des informations générales sur les tâches créées dans Kaspersky Security Center sont fournies dans l'Aide de Kaspersky Security Center.

Types de tâche.

Pour administrer l'application Kaspersky Endpoint Security, Kaspersky Security Center propose les tâches suivantes :

- *Analyse des logiciels malveillants*. Lors de l'exécution de la tâche, l'application vérifie les zones de l'appareil indiquées dans les paramètres de la tâche pour détecter les virus et les autres applications malveillantes.
- *Analyse des zones critiques*. Lors de l'exécution de la tâche, l'application analyse les secteurs d'amorçage, les objets de démarrage automatique, la mémoire des processus et la mémoire du noyau.
- *Analyse du conteneur*. Lors de l'exécution de cette tâche, l'application analyse les conteneurs et les images à la recherche de virus et d'autres applications malveillantes.
- *Inventaire*. Lors de l'exécution de la tâche, l'application obtient des informations sur tous les fichiers exécutables stockés sur les appareils et gère la Golden Image.
- *Vérification de l'intégrité du système*. Lors de l'exécution de la tâche, l'application confirme chaque modification d'objet via la comparaison de l'état actuel des objets surveillés à l'état d'origine, défini au préalable comme référence.
- *Ajout d'une clé*. Lors de l'exécution de la tâche, l'application ajoute la clé, y compris la clé de réserve, pour activer l'application.

- *Mise à jour*. Lors de l'exécution de la tâche, l'application met à jour les bases de données en fonction des paramètres de mise à jour configurés.
- *Annulation de la mise à jour des bases*. Lors de l'exécution de la tâche, l'application annule la dernière mise à jour des bases de données.

Gestion des tâches dans Web Console

Comment créer une tâche pour un groupe ou une sélection d'appareils dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Dans la première étape de l'Assistant, procédez comme suit :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

   b. Dans la liste déroulante **Type de tâche**, sélectionnez le type de tâche que vous souhaitez créer.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez comment vous souhaitez définir la zone d'action de la tâche. La zone d'action d'une tâche correspond aux appareils sur lesquels la tâche sera exécutée :

      - Sélectionnez l'option **Attribuer une tâche à un groupe d'administration** si la tâche doit être effectuée sur tous les appareils membres d'un groupe d'administration spécifique.
      - Sélectionnez l'option **Spécifier les adresses des appareils manuellement ou importer à partir de la liste** si la tâche doit être effectuée sur les appareils spécifiés.
      - Sélectionnez l'option **Attribuer une tâche à une sélection d'appareils** si la tâche doit être exécutée sur des appareils inclus dans la sélection d'appareils en fonction de critères prédéfinis. Pour créer une sélection d'appareils, consultez l'aide de Kaspersky Security Center.

   Passez à l'étape suivante de l'Assistant.

4. Selon la méthode que vous choisissez pour définir la portée d'une tâche, effectuez l'une des opérations suivantes :

   - Dans l'arborescence des groupes d'administration, cochez les cases en regard des groupes d'administration requis.
   - Dans la liste des appareils, cochez les cases en regard des appareils souhaités. Si les appareils dont vous avez besoin ne figurent pas dans la liste, vous pouvez les ajouter des manières suivantes :
     - À l'aide du bouton **Ajouter des appareils**. Vous pouvez ajouter des appareils par nom ou adresse IP, ajouter des appareils à partir d'une plage IP spécifiée ou sélectionner des appareils dans la liste des appareils détectés par le Serveur d'administration lors de l'interrogation du réseau local de l'organisation.
     - À l'aide du bouton **Importer des appareils à partir d'un fichier**. Pour importer, un fichier TXT avec une liste d'adresses d'appareils est utilisé, où chaque adresse doit être située sur une ligne distincte.
   - Dans la liste, sélectionnez le nom de la sélection contenant les appareils souhaités.

   Passez à l'étape suivante de l'Assistant.

5. Pour gérer les paramètres de la tâche immédiatement après sa création, à la dernière étape de l'Assistant, cochez la case **Ouvrir les détails de la tâche une fois la création terminée**. La tâche est créée avec les paramètres par défaut.

6. Quittez l'Assistant.

La nouvelle tâche apparaît dans la liste des tâches.

Comment créer une tâche locale dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour ce faire, cliquez sur le bouton **Afficher la hiérarchie** au-dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez créer une tâche et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, accédez à l'onglet **Tâches**.

   Une liste des tâches créées pour cet appareil s'ouvrira.

5. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

6. Dans la première étape de l'Assistant, procédez comme suit :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

   b. Dans la liste déroulante **Type de tâche**, sélectionnez le type de tâche que vous souhaitez créer.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

7. Pour gérer les paramètres de la tâche immédiatement après sa création, à la dernière étape de l'Assistant, cochez la case **Ouvrir les détails de la tâche une fois la création terminée**. La tâche est créée avec les paramètres par défaut.

8. Quittez l'Assistant.

La nouvelle tâche apparaît dans la liste des tâches.

Comment démarrer, arrêter, suspendre ou reprendre une tâche dans Web Console

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Exécutez une des actions suivantes :

   - Pour démarrer ou arrêter une tâche exécutée sur tous les appareils inclus dans un groupe d'administration donné, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre et sélectionnez le groupe d'administration dans la fenêtre qui s'affiche.

     La liste affichera uniquement les stratégies créées pour le groupe d'administration sélectionné.

   - Pour démarrer ou arrêter une tâche exécutée sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre et sélectionnez le nœud supérieur portant le nom du Serveur d'administration dans la fenêtre qui s'affiche.

     La liste affichera toutes les tâches créées sur le Serveur d'administration.

3. Dans la liste des tâches, cochez la case en regard du nom de la tâche souhaitée et cliquez sur le bouton de l'action souhaitée au-dessus de la liste des tâches.

> Il est impossible de suspendre et de reprendre la *tâche de mise à jour*. Vous pouvez uniquement l'arrêter ou la démarrer.

Gestion des tâches dans la Console d'administration

Comment créer une tâche pour un groupe ou une sélection d'appareils dans la Console d'administration

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez créer une tâche qui sera exécutée sur les appareils inclus dans le groupe d'administration sélectionné, dans l'arborescence de la console dans le dossier **Appareils administrés**, sélectionnez ce groupe d'administration, puis dans la zone de travail sélectionnez l'onglet **Tâches** et cliquez sur le bouton **Nouvelle tâche**.

     L'Assistant de création d'une tâche pour les appareils du groupe d'administration sélectionné démarre.

   - Si vous souhaitez créer une tâche qui sera exécutée sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console et cliquez sur le bouton **Nouvelle tâche** dans l'espace de travail.

     L'Assistant de création d'une tâche pour un ensemble d'appareils démarre.

2. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security et le type de tâche.

   Passez à l'étape suivante de l'Assistant.

3. Si vous créez une tâche pour un ensemble d'appareils, l'Assistant vous demandera de définir la zone d'action de la tâche. La zone d'action d'une tâche correspond aux appareils sur lesquels la tâche sera exécutée.

   a. Spécifiez la méthode de détermination de l'étendue de la tâche : sélectionnez les appareils dans la liste des appareils détectés par le Serveur d'administration ; définissez les adresses des appareils manuellement ; importez une liste d'appareils à partir d'un fichier ou spécifiez une sélection d'appareils préalablement configurée (pour plus de détails, consultez l'Aide de Kaspersky Security Center).

   b. En fonction de la méthode que vous avez spécifiée pour définir la portée dans la fenêtre qui s'ouvre, effectuez l'une des opérations suivantes :

      - Dans la liste des appareils détectés, précisez les appareils sur lesquels la tâche sera exécutée. Pour ce faire, cochez la case dans la liste à gauche du nom de l'appareil.
      - Cliquez sur le bouton **Ajouter** ou **Ajouter une plage IP** et spécifiez manuellement les adresses des appareils.
      - Cliquez sur le bouton **Importer** et dans la fenêtre qui s'ouvre, sélectionnez un fichier TXT contenant une liste d'adresses des appareils.
      - Cliquez sur le bouton **Parcourir** et dans la fenêtre qui s'ouvre, précisez le nom de la sélection contenant les appareils sur lesquels la tâche sera exécutée.

   Passez à l'étape suivante de l'Assistant.

4. Configurez les paramètres de tâche disponibles en suivant les instructions de l'Assistant.

5. Saisissez un nom pour la nouvelle tâche et passez à l'étape suivante de l'Assistant.

6. Si vous souhaitez que la tâche s'exécute immédiatement une fois l'Assistant terminé, cochez la case **Exécuter la tâche une fois l'Assistant terminé**.

7. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

Comment créer une tâche locale dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, sélectionnez la section **Tâches**.

   Une liste des tâches créées pour cet appareil s'ouvrira.

5. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

6. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security et le type de tâche.

   Passez à l'étape suivante de l'Assistant.

7. Saisissez un nom pour la nouvelle tâche et configurez les paramètres de tâche disponibles en suivant les instructions de l'Assistant.

8. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

Comment démarrer, arrêter, suspendre ou reprendre une tâche dans la Console d'administration

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur des appareils faisant partie d'un groupe d'administration spécifique, sélectionnez ce groupe d'administration dans l'arborescence de la console, puis sélectionnez l'onglet **Tâches** dans l'espace de travail.

     Une liste des tâches créées pour le groupe d'administration sélectionné s'ouvrira.

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console.

     Une liste de toutes les tâches créées sur le Serveur d'administration s'ouvrira.

2. Dans la liste des tâches, sélectionnez la tâche souhaitée, ouvrez le menu contextuel de la tâche et sélectionnez l'action que vous souhaitez effectuer.

   Il est impossible de suspendre et de reprendre la *tâche de mise à jour*. Vous pouvez uniquement l'arrêter ou la démarrer.

Dans la liste des tâches, vous pouvez surveiller l'exécution d'une tâche : afficher l'état de la tâche et statistiques d'exécution des tâches sur les appareils. Vous pouvez également créer une sélection d'événements pour surveiller l'exécution des tâches. Pour plus de détails sur la sélection des événements, consultez l'Aide de Kaspersky Security Center.

Les résultats de l'exécution des tâches sont également enregistrés localement sur l'appareil et dans les rapports de Kaspersky Security Center.

Particularités de la gestion et de l'exécution des tâches

- La tâche pour les sélections d'appareils est exécutée uniquement sur les appareils spécifiés dans la tâche. Si de nouveaux appareils sont ajoutés à la sélection d'appareils pour laquelle une tâche a été créée, cette tâche ne sera pas exécutée sur ces appareils. Dans ce cas, vous devez créer une nouvelle tâche ou modifier la tâche existante.

- Les tâches sont exécutées uniquement si l'application Kaspersky Endpoint Security est en cours d'exécution sur l'appareil.

- Si l'appareil est sous le contrôle de stratégie, l'affichage et la gestion des tâches créées dans Kaspersky Security Center peuvent ne pas être disponibles via la ligne de commande ou via l'interface graphique de l'application.

- Pour l'application Kaspersky Endpoint Security dans Kaspersky Security Center, vous pouvez créer tous les types de tâches. L'application et l'exécution des tâches sur un appareil protégé sont déterminées par le mode de l'application sur l'appareil. Par exemple, les tâches *Ajouter une clé*, *Mise à jour* et *Annulation de la mise à jour des bases* ne sont pas appliquées sur l'appareil si l'application fonctionne en mode Light Agent.

Connexion et déconnexion de Web Console et de Cloud Console

Kaspersky Security Center Web Console

Pour entrer dans Web Console, vous devez connaître l'adresse Internet du Serveur d'administration et le numéro de port. Ces deux éléments sont définis lors de l'installation de Web Console, (le port 8080 est utilisé par défaut). Il faut également activer JavaScript dans le navigateur.

Vous pouvez vous connecter à Kaspersky Security Center Web Console à l'aide de l'une des méthodes suivantes :

- Authentification de domaine (Single Sign-On)
- Nom d'utilisateur et mot de passe d'un utilisateur du domaine
- Nom d'utilisateur et mot de passe d'un utilisateur interne

Pour en savoir plus sur la connexion à Kaspersky Security Center Web Console et la déconnexion de celle-ci, consultez l'Aide de Kaspersky Security Center.

Pour vous connecter à Web Console en indiquant un nom d'utilisateur et un mot de passe :

1. Dans votre navigateur, accédez à :

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   La page de sélection du Serveur d'administration s'ouvre.

2. Si vous avez ajouté plusieurs serveurs d'administration de confiance, sélectionnez dans la liste le Serveur d'administration auquel vous souhaitez vous connecter.

   Si vous n'avez ajouté qu'un seul Serveur d'administration, la liste des Serveurs d'administration ne s'affiche pas.

   Le navigateur est redirigé vers `https://<Administration Server address>:4444`.

3. Saisissez le nom d'utilisateur et le mot de passe de votre compte.

   Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois.

4. Cliquez sur le bouton **Entrer**.

   Si le Serveur d'administration ne répond pas ou si vous avez saisi des identifiants incorrects, un message d'erreur s'affiche.

5. Saisissez le code de sécurité à usage unique généré dans l'application d'authentification sur votre appareil mobile.

   Si vous vous connectez pour la première fois, configurez l'authentification en deux étapes pour votre compte.

Une fois connecté, un tableau de bord s'affiche avec la dernière langue et le dernier thème utilisés.

Pour en savoir plus sur l'interface de Web Console, consultez l'aide de Kaspersky Security Center.

Pour quitter Web Console :

dans le coin inférieur gauche de l'écran, sélectionnez **<Nom du compte 'utilisateur>** → **Quitter**.

Web Console se ferme et la page de connexion s'affiche.

Kaspersky Security Center Cloud Console

Pour Kaspersky Security Center Cloud Console, utilisez un jeton web pour vous connecter à votre compte dans le portail Cloud Console.

Pour en savoir plus sur Kaspersky Security Center Cloud Console, consultez la documentation de Kaspersky Security Center Cloud Console.

Administrer l'application via la ligne de commande

À l'aide de la ligne de commande, vous pouvez installer, désinstaller, démarrer et arrêter Kaspersky Endpoint Security sur l'appareil, ainsi que gérer l'application localement.

Modules et tâches

Le fonctionnement des modules fonctionnels de l'application est assuré par les *tâches locales de Kaspersky Endpoint Security* qui s'exécutent dans le système d'exploitation. Pour activer ou désactiver un module fonctionnel de l'application sur un appareil, vous devez démarrer ou arrêter la tâche Kaspersky Endpoint Security correspondante sur la ligne de commande.

Pour analyser un appareil une fois, vous devez également démarrer la tâche Kaspersky Endpoint Security correspondante.

Pour gérer les paramètres d'un module fonctionnel sur un appareil ou les paramètres d'analyse d'un appareil, vous devez gérer les paramètres de la tâche Kaspersky Endpoint Security correspondante.

Paramètres généraux

Outre les paramètres propres à chaque tâche de Kaspersky Endpoint Security, il existe des paramètres généraux :

- Paramètres généraux d'analyse du conteneur. Utilisés lors de l'analyse des conteneurs et des espaces de noms en temps réel (Surveillance des conteneurs).
- Paramètres d'analyse du trafic réseau. Utilisés par les modules Protection contre les menaces Internet, Protection contre les menaces réseau, Protection contre les menaces par emails et Contrôle Internet.
- Paramètres généraux de l'application. Ces paramètres régissent le fonctionnement de l'application dans son ensemble et celui de fonctions individuelles.

Commandes d'administration

Vous pouvez gérer les tâches et les paramètres de Kaspersky Endpoint Security sur la ligne de commande à l'aide des *utilitaires kesl-control*.

Seules les tâches définies par l'utilisateur peuvent être créées ou supprimées. Les tâches prédéfinies ne peuvent pas être créées ni supprimées.

Selon le mode de fonctionnement de l'application, vous pouvez créer les types suivants de tâches définies par l'utilisateur :

- mode standard : *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* et *InventoryScan* ;
- Mode Light Agent : *ODS*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Vous pouvez démarrer et arrêter toutes les tâches prédéfinies et les tâches définies par l'utilisateur, à l'exception des tâches de type *License*.

Vous pouvez suspendre et reprendre les tâches *ODS*, *ODFIM* et *InventoryScan*.

Tâches locales de Kaspersky Endpoint Security

Les tâches suivantes peuvent être utilisées pour administrer Kaspersky Endpoint Security en ligne de commande, comme indiqué dans le tableau ci-dessous :

Chaque tâche de l'application possède un nom utilisé sur la ligne de commande, un identifiant et un type.

Les identifiants sont uniques pour toutes les tâches, y compris celles à distance. L'application ne réutilise pas les ID de tâche supprimés. L'ID de la nouvelle tâche est le numéro qui suit l'ID de la dernière tâche créée.

Les noms de tâche ne sont pas sensibles à la casse.

Les *tâches prédéfinies* sont créées lors de l'installation de l'application. Ces tâches ne peuvent pas être supprimées. Chaque tâche prédéfinie a un nom et un identifiant réservés.

Les tâches que vous créez lorsque vous travaillez avec une application sont appelées *tâches utilisateur*. Vous spécifiez les noms de ces tâches lors de la création d'une tâche. L'application définit et attribue des identifiants de tâche utilisateur à une tâche lors de sa création. Les IDs des tâches personnalisées commencent à 100.

Pendant que l'application est en cours d'exécution, elle crée des *tâches d'analyse temporaires*. Les noms et les identifiants des tâches temporaires sont spécifiés par l'application. Les tâches temporaires sont automatiquement supprimées une fois terminées.

Tâches de l'application

Tâche	Description de la tâche	Nom de la tâche dans la ligne de commande	ID de la tâche	Type de tâche
Protection contre les fichiers malicieux	Cette tâche vous permet d'activer ou de désactiver la protection contre les menaces de fichiers en temps réel et définit les paramètres du module Protection contre les menaces de fichiers. Si la Protection contre les fichiers malicieux est activée, la tâche s'exécute automatiquement au démarrage de l'application	File_Threat_Protection	1	OAS
Analyse des logiciels malveillants :	Cette tâche vous permet d'analyser les objets du système de fichiers à la recherche de logiciels malveillants à la demande et de définir les paramètres d'analyse. Vous pouvez utiliser cette tâche pour effectuer une analyse complète ou personnalisée des appareils.	Scan_My_Computer	2	ODS
Analyse des logiciels malveillants (personnalisée)		défini par l'utilisateur	à partir de 100	ODS
Analyse personnalisée des fichiers	Cette tâche est destinée à configurer et à stocker les paramètres utilisés lors de l'analyse des fichiers et répertoires spécifiés à l'aide de la commande `kesl-control --scan-file`. Suite à l'exécution de la commande, l'application crée et exécute une tâche d'analyse de fichiers temporaire.	Scan_File	3	ODS
Analyse des zones critiques.	Cette tâche vous permet d'analyser les zones critiques du système d'exploitation à la demande et de définir les paramètres d'analyse.	Critical_Areas_Scan	4	ODS
Mise à jour.	À l'aide de cette tâche, vous pouvez mettre à jour les bases de données et les modules de l'application selon une planification et à la demande et configurer les paramètres de mise à jour.	Update	6	Update
Mise à jour (personnalisée)		défini par l'utilisateur	à partir de 100	Update
Annulation de la mise à jour.	À l'aide de cette tâche, vous pouvez annuler la dernière mise à jour des bases de données et des modules de l'application.	Rollback	7	Rollback
Annulation de la mise à jour des bases (personnalisée)		défini par l'utilisateur	à partir de 100	Rollback
Licence	Cette tâche offre la possibilité d'activer une application installée sur l'appareil. La tâche démarre automatiquement au démarrage de l'application et est située en permanence dans la mémoire vive de l'appareil. La tâche n'a pas de paramètres ; les clés de licence sont gérées à l'aide de commandes de gestion spéciales . La tâche ne peut pas être démarrée, arrêtée ou supprimée.	License	9	License
vérification de l'intégrité du système.	Cette tâche vous permet de vérifier les modifications apportées aux fichiers et répertoires que vous avez inclus dans la zone de surveillance en comparant l'état actuel de l'objet surveillé avec un état précédemment capturé.	System_Integrity_Monitoring	11	OAFIM
Vérification de l'intégrité du système (tâche définie par l'utilisateur)		défini par l'utilisateur	à partir de 100	ODFIM

Tâche	Description de la tâche	Nom de la tâche dans la ligne de commande	ID de la tâche	Type de tâche
Gestion du pare-feu	Cette tâche vous permet d'activer ou de désactiver la gestion du pare-feu et de définir les paramètres de surveillance des connexions réseau sur l'appareil.	Firewall_Management	12	Firewall
Protection contre le chiffrement	Cette tâche vous permet d'activer ou de désactiver la protection des fichiers contre le chiffrement malveillant à distance et définit les paramètres du module Protection contre le chiffrement.	Anti_Cryptor	13	AntiCryptor
Protection contre les menaces Internet	Cette tâche permet d'activer ou de désactiver la Protection contre les menaces Internet et définit les paramètres du module Protection contre les menaces Internet. Si la Protection contre les menaces Internet est activée, la tâche s'exécute automatiquement au démarrage de l'application	Web_Threat_Protection	14	WTP
Contrôle des appareils	Cette tâche vous permet d'activer ou de désactiver le contrôle des appareils et définit les paramètres du module Contrôle des appareils. Si le Contrôle des appareils est activé, la tâche s'exécute automatiquement au démarrage de l'application.	Device_Control	15	DeviceControl
Analyse des disques amovibles.	Cette tâche vous permet de surveiller en temps réel la connexion des disques amovibles à l'appareil et définit les paramètres d'analyse des disques amovibles et de leurs secteurs de démarrage pour détecter la présence de logiciels malveillants.	Removable_Drives_Scan	16	RDS
Protection contre les menaces réseau	Cette tâche vous permet d'activer ou de désactiver la protection contre les menaces réseau et définit les paramètres de fonctionnement du module Protection contre les menaces réseau.	Network_Threat_Protection	17	NTP
Analyse du conteneur	Cette tâche vous permet d'analyser des conteneurs et des images à la demande et définit les paramètres d'analyse.	Container_Scan	18	ContainerScan
Analyse du conteneur (personnalisée)		défini par l'utilisateur	à partir de 100	ContainerScan
Analyse personnalisée du conteneur	Cette tâche est destinée à configurer et à stocker les paramètres utilisés lors de l'analyse des conteneurs et images spécifiés à l'aide de la commande `kesl-control [-T] --scan-container`. Suite à l'exécution de la commande, l'application crée et exécute une tâche temporaire d'analyse du conteneur.	Custom_Container_Scan	19	ContainerScan
Détection comportementale	Cette tâche vous permet de surveiller l'activité des applications malveillantes sur le système d'exploitation. Si la Détection comportementale est activée, la tâche s'exécute automatiquement au démarrage de l'application.	Behavior_Detection	20	BehaviorDetection
Contrôle des applications	Cette tâche vous permet d'activer ou de désactiver le Contrôle des applications et définit les paramètres du module Contrôle des applications.	Application_Control	21	AppControl
Inventaire	Cette tâche permet d'obtenir des informations sur tous les fichiers exécutables des applications installées sur l'appareil et de gérer la catégorie d'applications Golden Image.	Inventory_Scan	22	InventoryScan
Inventaire (personnalisée)		défini par l'utilisateur	à partir de 100	InventoryScan

Tâche	Description de la tâche	Nom de la tâche dans la ligne de commande	ID de la tâche	Type de tâche
Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises).	Cette tâche permet d'activer ou de désactiver l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA) et de gérer les paramètres d'intégration.	KATAEDR	24	KATAEDR
Contrôle Internet	Cette tâche vous permet d'activer ou de désactiver le Contrôle Internet et définit les paramètres du module Contrôle Internet.	Web_Control	26	WebControl
Intégration avec Sandbox	Cette tâche vous permet d'activer ou de désactiver l'intégration avec Sandbox et de définir les options d'intégration.	Standalone_Sandbox	29	StandaloneSandbox
Prévention de l'exécution des objets (EDR Expert (on-premises))	Cette tâche vous permet d'activer et de désactiver l'utilisation des règles de prévention de l'exécution de Endpoint Detection and Response Expert (on-premises), ainsi que d'afficher la liste de ces règles.	KATAEDR_Prevention	30	KATAEDRPrevention
Intégration avec Kaspersky Network Detection and Response (KATA).	Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Network Detection and Response (KATA) et de définir les paramètres d'intégration.	KATANDR	31	KATANDR
Prévention du lancement des objets (EDR Optimum)	Cette tâche vous permet d'activer ou de désactiver l'utilisation des règles d'interdiction de lancer des objets du module Endpoint Detection and Response Optimum et d'afficher une liste de ces règles.	EDRO_Prevention	32	Prevention
Intégration avec KUMA	Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Unified Monitoring and Analysis Platform et de définir les paramètres d'intégration.	KUMA	33	KUMA
Protection contre les menaces par emails	Cette tâche permet d'analyser les pièces jointes des messages électroniques entrants et sortants à la recherche de virus et d'autres applications présentant une menace. Si la Protection contre les menaces par emails est activée, la tâche s'exécute automatiquement au démarrage de l'application	Mail_Monitoring	35	MailMonitoring
Protection BadUSB	Cette tâche vous permet d'empêcher la connexion d'appareils USB infectés imitant un clavier à un appareil client.	Bad_USB	37	BadUSB
Intégration de Kaspersky Endpoint Detection and Response Expert (cloud)	Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) et de définir les paramètres d'intégration.	EDRExpertCloud	39	EDRExpertCloud

Modification des paramètres d'une tâche

Vous pouvez modifier les paramètres de toutes les tâches définies par l'utilisateur et de toutes les tâches prédéfinies, à l'exception des tâches de type *Annulation de la mise à jour des bases* et *License* (ces tâches n'ont aucun paramètre). Si l'application est utilisée en mode Light Agent, les paramètres de la tâche prédéfinie *Update* ne peuvent pas non plus être modifiés.

Pour les tâches de type *OAS*, *ODS*, *OAFIM*, *ODFIM* et *AntiCryptor*, vous pouvez ajouter ou supprimer des zones d'analyse et des zones d'exclusion.

Vous pouvez modifier les paramètres des tâches des manières suivantes :

- À l'aide d'un fichier de configuration. Cette méthode permet de modifier tous les paramètres de la tâche simultanément. Vous pouvez obtenir un fichier de configuration à modifier à l'aide de la commande qui affiche les paramètres de la tâche.

- À l'aide des options de ligne de commande au format <nom du paramètre>=<valeur du paramètre>. Cette méthode permet de modifier des paramètres individuels de la tâche. Vous pouvez consulter les valeurs actuelles des paramètres de la tâche à l'aide de la commande qui affiche les paramètres de la tâche.

Certaines tâches disposent également de commandes de contrôle distinctes qui vous permettent de modifier les paramètres de la tâche.

Comment afficher les valeurs actuelles des paramètres de la tâche

Vous pouvez afficher les valeurs actuelles des paramètres de la tâche sur la console ou dans un fichier de configuration. Vous pouvez ensuite modifier ce fichier afin de changer les paramètres de la tâche.

```
Afficher les valeurs actuelles des paramètres de la tâche sur la console

kesl-control --get-settings <task ID|name>
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

```
Afficher les valeurs actuelles des paramètres de la tâche dans un fichier de configuration

kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

Où :

- `--file <path to configuration file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de la tâche. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Comment modifier les paramètres d'une tâche à l'aide d'un fichier de configuration :

1. Exportez les paramètres de la tâche vers le fichier de configuration à l'aide de la commande suivante :

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   où :

   - `--file <path to configuration file>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.

   - Spécifiez l'option `--json` si vous souhaitez exporter les paramètres vers un fichier de configuration au format JSON. Si l'option `--json` n'est pas spécifiée, l'application exporte les paramètres vers un fichier INI.

2. Ouvrez le fichier de configuration obtenu, modifiez les paramètres si nécessaire, puis enregistrez vos modifications.

   Pour les tâches de type *OAS*, *ODS*, *OAFIM*, *ODFIM* et *AntiCryptor*, vous pouvez ajouter ou supprimer des zones d'analyse et des zones d'exclusion.

   Si vous souhaitez ajouter une zone d'analyse, ajoutez la section `[ScanScope.item_#]` au fichier avec les paramètres suivants :

   - `AreaDesc` : description de la zone d'analyse, qui contient des informations supplémentaires sur cette zone.
   - `UseScanArea` : activer l'analyse de la zone spécifiée.
   - `Path` est le chemin d'accès au répertoire contenant les objets à analyser. Vous pouvez spécifier le chemin d'accès à un répertoire local ou activer l'analyse des répertoires distants montés sur l'appareil client.
   - `AreaMask.item_#` : restriction de la zone d'analyse. Vous pouvez spécifier un masque pour les noms des fichiers à analyser. Par défaut, l'analyse est activée pour tous les objets dans la zone d'analyse. Vous pouvez spécifier plusieurs éléments `AreaMask.item_#`.

   Si vous souhaitez ajouter une zone d'exclusion, ajoutez une section `[ExcludedFromScanScope.item_#]` au fichier avec les paramètres suivants :

   - `AreaDesc` : spécifie la description de la zone d'exclusion, qui contient des informations supplémentaires sur la zone d'exclusion.
   - `UseScanArea` : activer l'exclusion de la zone spécifiée.
   - `Path` est le chemin d'accès au répertoire contenant les objets à exclure. Vous pouvez spécifier le chemin d'accès à un répertoire local ou exclure les répertoires distants montés sur l'appareil client. Les valeurs de paramètres possibles dépendent du type de tâche.
   - `AreaMask.item_#` : limitation de la zone d'exclusion. Vous pouvez spécifier un masque pour les noms des fichiers que vous souhaitez exclure de la portée de l'analyse. Par défaut, tous les objets de portée sont exclus.

     Exemple

     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   Vous pouvez spécifier plusieurs sections `[ScanScope.item_#]` et `[ExcludedFromScanScope.item_#]`. L'application traite les zones par ordre croissant d'index d'élément.

3. Exécutez la commande:

   ```
   kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
   ```

où :

- `<task ID/name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--file <path to configuration file>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de tâche spécifiées dans le fichier seront importées dans l'application.

Si vous modifiez la liste d'autorisation de la tâche Contrôle des applications ou si vous interdisez le lancement de toutes les applications et/ou des applications ayant un impact sur le fonctionnement de Kaspersky Endpoint Security, il faut exécuter la commande `--set-settings` avec la clé `--accept`.

Comment modifier des paramètres individuels de la tâche à l'aide des options de ligne de commande

Exécutez la commande :

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `<setting name >=<setting value>` correspond au nom et à la valeur d'un paramètre de tâche. Vous pouvez obtenir les valeurs actuelles des paramètres de la tâche à l'aide de la commande d'affichage des paramètres de la tâche.

Les valeurs des paramètres spécifiés de la tâche seront modifiées.

Si vous modifiez la liste d'autorisation de la tâche Contrôle des applications ou si vous interdisez le lancement de toutes les applications et/ou des applications ayant un impact sur le fonctionnement de Kaspersky Endpoint Security, il faut exécuter la commande `--set-settings` avec la clé `--accept`.

Comment ajouter ou supprimer une zone d'analyse à l'aide des options de ligne de commande

```
Ajouter une zone d'analyse à l'aide des options de ligne de commande
```

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `<path>` est le chemin d'accès au répertoire contenant les objets à analyser.

Cette commande ajoute une nouvelle section `[ScanScope.item_#]` aux paramètres de la tâche. L'application analyse les objets situés dans le répertoire défini par le paramètre `Path`. Les autres paramètres de la zone d'analyse prennent leurs valeurs par défaut.

Si les paramètres de la tâche ont déjà une section `[ScanScope.item_#]` avec la valeur spécifiée du paramètre `Path`, la section en double n'est pas ajoutée.

Si le paramètre `UseScanArea` a reçu la valeur `No`, il prend la valeur `Yes` après l'exécution de la commande et les objets situés dans ce répertoire sont analysés.

Exemple d'ajout du répertoire /home à la zone d'analyse pour une tâche avec l'ID=100

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/home
```

Les paramètres suivants de la zone d'analyse seront ajoutés à la tâche :

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Supprimer une zone d'analyse à l'aide des options de ligne de commande

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

Cette commande supprime la section `[ScanScope.item_#]`, qui contient le chemin d'accès spécifié, des paramètres de la tâche. L'application n'analysera pas les objets dans le répertoire spécifié.

Comment ajouter ou supprimer une zone d'exclusion à l'aide des options de ligne de commande

Ajouter une zone d'exclusion à l'aide des options de ligne de commande

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `<path>` est le chemin d'accès au répertoire contenant les objets à exclure.

Cette commande ajoute une nouvelle section `[ExcludedFromScanScope.item_#]` aux paramètres de la tâche. L'application exclura des analyses les objets du répertoire spécifié par le paramètre `Path`. Les autres paramètres de la zone d'exclusion prennent leurs valeurs par défaut.

Si les paramètres de la tâche ont déjà une section `[ExcludedFromScanScope.item_#]` avec la valeur spécifiée du paramètre `Path`, la section en double n'est pas ajoutée.

Si le paramètre `UseScanArea` a reçu la valeur `No`, il prend la valeur `Yes` après l'exécution de la commande et les objets situés dans ce répertoire sont exclus de l'analyse.

Supprimer une zone d'exclusion à l'aide des options de ligne de commande

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

Cette commande supprime la section `[ExcludedFromScanScope.item_#]`, qui contient le chemin d'accès spécifié, des paramètres de la tâche. L'application n'exclura pas les objets du répertoire spécifié de l'analyse.

Comment restaurer les paramètres par défaut de la tâche

Exécutez la commande :

```
kesl-control --set-settings <task ID|name> --set-to-default
```

Où `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

L'application substituera les valeurs des paramètres par les valeurs par défaut.

Configuration de la planification des tâches

Selon le mode de fonctionnement de l'application, vous pouvez configurer une planification pour les types de tâches suivants :

- mode standard : *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* et *InventoryScan* ;
- Mode Light Agent : *ODS*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Vous pouvez modifier la planification des tâches des manières suivantes :

- À l'aide d'un fichier de configuration. Cette méthode permet de modifier tous les paramètres de planification des tâches en même temps. Vous pouvez obtenir un fichier de configuration à modifier à l'aide de la commande qui affiche les paramètres de planification.
- À l'aide des options de ligne de commande au format <nom du paramètre>=<valeur du paramètre>. Cette méthode permet de modifier individuellement les paramètres de planification des tâches. Vous pouvez consulter les valeurs actuelles des paramètres de la tâche à l'aide de la commande qui affiche les paramètres de planification.

Comment afficher les paramètres actuels de planification

Vous pouvez afficher les valeurs actuelles des paramètres de planification de lancement des tâches sur la console ou dans un fichier de configuration. Vous pouvez ensuite modifier ce fichier pour changer les paramètres.

```
Afficher les paramètres actuels de planification de la tâche dans la console

kesl-control --get-schedule <task ID|name> [--json]
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas la clé --json, les paramètres seront affichés au format INI.

```
Exporter les paramètres actuels de planification de la tâche dans un fichier de configuration

kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

Où `--file <path to configuration file>` correspond au chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de planification de la tâche. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

```
Exemple d'exportation des paramètres de planification de la tâche de mise à jour dans un fichier nommé update_schedule.ini et d'enregistrement du fichier créé dans le répertoire actif
```

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

```
Exemple d'affichage de la planification de la tâche de mise à jour dans le terminal
```

```
kesl-control --get-schedule 6
```

Comment configurer la planification de la tâche à l'aide d'un fichier de configuration

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--file <path to configuration file>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de planification de la tâche.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

```
Exemple d'importation des paramètres de planification depuis le fichier de configuration /home/test/on_demand_schedule.ini dans la tâche portant l'ID=2
```

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Comment modifier les paramètres de planification de la tâche à l'aide d'options de ligne de commande :

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `<setting name>=<setting value>` correspond au nom et à la valeur d'un paramètre de planification des tâches.

```
Exemple de configuration d'une tâche pour qu'elle s'exécute toutes les 10 heures
```

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

```
Exemple de configuration d'une tâche pour qu'elle s'exécute toutes les 10 minutes
```

```
RuleType=Minutely
RunMissedStartRules=No
```

```
StartTime=23:10:00;10
RandomInterval=0
```

Exemple de configuration d'une tâche pour qu'elle s'exécute le 15 de chaque mois

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

Exemple de configuration d'une tâche pour qu'elle s'exécute tous les mardis

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

Exemple de configuration d'une tâche pour qu'elle s'exécute tous les 11 jours

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Gestion des paramètres généraux de l'application

Les paramètres généraux de l'application déterminent le fonctionnement de l'application dans son ensemble et le fonctionnement des fonctions individuelles. Avec les paramètres généraux, vous pouvez :

- Configurez l'utilisation de Kaspersky Security Network et la version allégée des bases de données antimalware dans l'application.
- Configurer l'utilisation d'un serveur proxy dans le fonctionnement de l'application.
- Sélectionner le mode d'interception des opérations sur les fichiers (bloquer/ne pas bloquer les fichiers pendant l'analyse).
- Configurer les exclusions d'analyse des points de montage (exclusions globales).
- Configurez les exclusions de l'analyse de la mémoire des processus.
- Activez ou désactivez la Surveillance des conteneurs en temps réel.
- Activer ou désactiver la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.
- Activer ou désactiver l'intégration avec Kaspersky Managed Detection and Response.
- Configurer l'utilisation des journaux d'événements.
- Configurez une limite d'utilisation des ressources du processeur par les tâches d'analyse (de type ODS).
- Limiter le nombre de tâches d'analyse personnalisée qu'un utilisateur non privilégié peut exécuter simultanément.

Vous pouvez gérer les paramètres généraux de l'application à l'aide des commandes de gestion spéciales des manières suivantes :

- À l'aide d'un fichier de configuration. Cette méthode permet de modifier tous les paramètres généraux simultanément. Vous pouvez obtenir un fichier de configuration à modifier à l'aide de la commande d'affichage des paramètres généraux.

- À l'aide des options de ligne de commande au format <nom du paramètre>=<valeur du paramètre>. Cette méthode permet de modifier des paramètres individuels. Vous pouvez obtenir les valeurs actuelles des paramètres à l'aide de la commande d'affichage des paramètres généraux.

Procédure d'affichage des valeurs actuelles des paramètres généraux de l'application

Vous pouvez afficher les valeurs actuelles des paramètres généraux de l'application dans la console ou dans un fichier de configuration. Vous pouvez ensuite utiliser ce fichier pour modifier les paramètres.

```
Afficher les valeurs actuelles des paramètres généraux de l'application dans la console
```

```
kesl-control --get-app-settings [--json]
```

Où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

```
Afficher les valeurs actuelles des paramètres généraux de l'application dans un fichier de configuration
```

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Où `--file <path to configuration file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez afficher les paramètres généraux de l'application. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

```
Exemple d'écriture des paramètres généraux de l'application dans le fichier kesl_config.ini du répertoire actuel
```

```
kesl-control --get-app-settings --file kesl_config.ini
```

Procédure de modification des paramètres d'une tâche à l'aide d'un fichier de configuration :

1. Affichez les paramètres généraux de l'application dans un fichier de configuration à l'aide de la commande `kesl-control --get-app-settings`.

2. Ouvrez le fichier de configuration obtenu, modifiez les paramètres si nécessaire, puis enregistrez vos modifications.

3. Exécutez la commande:

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

   où :

   - `--file <path to configuration file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux de l'application. Si vous supprimez un paramètre dans le fichier de configuration, la valeur par défaut de ce paramètre sera affichée après l'exécution de la commande.

   - `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres généraux spécifiées dans le fichier seront importées dans l'application.

Exemple d'importation des paramètres généraux dans l'application depuis le fichier de configuration /home/test/kesl_config.ini

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Procédure de modification des paramètres généraux à l'aide des options de ligne de commande

Modifier les paramètres généraux à l'aide des options de ligne de commande

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

Où `<setting name>=<setting value>` est le nom et la valeur d'un paramètre général de l'application.

Les valeurs des paramètres généraux spécifiés seront modifiées.

Exemple de définition d'un faible niveau de détail pour le fichier de traçage

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Exemple d'ajout d'une exclusion de point de montage de l'interception des opérations sur les fichiers

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Utilisation du filtre pour limiter les résultats des requêtes

Un filtre permet de limiter les résultats d'une requête lors de l'exécution de commandes de gestion de l'application. Les conditions du filtre sont spécifiées à l'aide d'une ou plusieurs *expressions logiques* combinées à l'aide de l'opérateur logiques `and`. Les conditions du filtrage doivent être placées entre guillemets :

Vous pouvez utiliser un filtre aux fins suivantes :

Afficher des informations sur certains événements actuels de l'application

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Afficher des informations sur certains événements de l'application dans le journal des événements

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Afficher des informations sur certains objets dans la Sauvegarde

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Supprimer certains objets de la Sauvegarde

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Où :

- `<field>` est le nom du champ de la base de données.
- `<comparison operator>` est l'une des opérations de comparaison suivantes :
  - `>` : supérieur à.
  - `<` signifie « inférieur à »
  - `like` correspond à la valeur spécifiée. Lors de la spécification d'une valeur, vous pouvez utiliser des masques % : par exemple, l'expression logique `"FileName like '%etc%'"` définit la restriction « contient le texte 'etc' dans le champ FileName »

    L'opération de comparaison `like` fonctionne uniquement avec les champs stockés dans la base de données au format texte. L'opération `like` ne fonctionne pas avec les champs contenant des dates, des heures, des nombres ou d'autres types de données non textuels.

  - `==` : égal à.
  - `!=` : pas égal à.
  - `>=` : supérieur ou égal à.
  - `<=` signifie « inférieur ou égal à »

- `<value>` est la valeur du champ. La valeur doit être spécifiée entre guillemets simples (').

  Vous pouvez spécifier la valeur de date dans le système d'horodatage UNIX™ (nombre de secondes depuis le 1er janvier 1970, 00:00:00 (UTC)) ou au format AAAA-MM-JJ hh:mm:ss. La valeur de date et d'heure est spécifiée par l'utilisateur et affichée par l'application dans l'heure locale de l'utilisateur.

Exemple de sortie des informations sur les événements qui contiennent le texte « etc » dans le champ FileName

```
kesl-control -E --query "FileName like '%etc%'"
```

Exemple de sortie des informations sur les événements de type ThreatDetected

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Exemple de sortie des informations sur les événements de type ThreatDetected générés par les tâches de type ODS

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Exemple de sortie des informations sur les événements générés après la date spécifiée dans le système d'horodatage UNIX (le nombre de secondes écoulées depuis 00:00:00 (UTC), le 1er janvier 1970)

```
kesl-control -E --query "Date > '1583425000'"
```

Exemple de sortie des informations sur les événements générés après la date spécifiée au format YYYY-MM-DD hh:mm:ss

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

Exemple de sortie des informations sur les fichiers dans la Sauvegarde qui ont un niveau de gravité Élevé

```
kesl-control -B --query "DangerLevel == 'High'"
```

Exportation et importation des paramètres de l'application

Kaspersky Endpoint Security permet d'exporter et d'importer tous les paramètres de l'application pour le dépannage, la vérification des paramètres ou pour simplifier la configuration de l'application sur les appareils utilisateurs.

Accordez l'accès au fichier de configuration uniquement aux utilisateurs de confiance. Avant d'importer les paramètres dans l'application, vérifiez les chemins d'accès aux répertoires, aux fichiers de configuration, aux fichiers exécutables et à la quarantaine. N'importez pas de fichiers de configuration provenant de sources non fiables. La compromission du fichier de configuration pourrait affecter la sécurité, l'intégrité ou le fonctionnement de l'infrastructure de votre organisation, ainsi que les données des utilisateurs.

Paramètres d'exportation

Lorsque vous exportez les paramètres, tous les paramètres de l'application (y compris les paramètres généraux de l'analyse du conteneur, les paramètres d'analyse du trafic réseau, les paramètres généraux de l'application et les paramètres des tâches) sont enregistrés dans le fichier de configuration. Vous pouvez ensuite utiliser ce fichier de configuration pour importer les paramètres dans l'application.

Exportation des paramètres de l'application

```
kesl-control --export-settings --file <configuration file path> [--json]
```

Où :

- `--file <configuration file path>` est le chemin d'accès complet au fichier de configuration dans lequel vous souhaitez enregistrer les paramètres de l'application.
- `--json` indique que les paramètres doivent être exportés vers le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'exportation se fera vers un fichier INI.

Importation des paramètres

1. Exécutez la commande:

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

Où :

- `--file <configuration file path>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de l'application.
- `--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

2. Redémarrez l'application.

Particularités et restrictions liées à l'exportation et à l'importation des paramètres

- Lors de l'importation ou de l'exportation de paramètres, l'application doit être en cours d'exécution.
- Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent, les paramètres de la tâche prédéfinie de type `Update` ne peuvent pas être exportés ni importés.
- Si la modification des paramètres est interdite par la stratégie, l'importation des paramètres n'est pas disponible.
- Si vous importez dans une version plus récente des paramètres exportés depuis une ancienne version de l'application, les paramètres qui n'existaient pas dans l'ancienne version sont définis sur les valeurs par défaut.
- Vous ne pouvez pas importer les paramètres d'une version plus récente vers une version plus ancienne.
- Certains paramètres de stratégie et de tâche ne peuvent pas être importés depuis les versions 12.3 et 12.4 du plug-in Internet de l'application vers la version 12.5 de l'application. La restriction s'applique aux paramètres de stratégie et de tâche suivants :
  - Zone de protection et zone d'exclusion de la Protection contre les fichiers malicieux et de la Protection contre le chiffrement
  - Exclusions de processus de l'analyse par l'Analyse comportementale
  - Appareils de confiance pour le Contrôle des appareils
  - Zone d'analyse et zone d'exclusion du Contrôle de l'intégrité du système
  - Règles du Contrôle Internet
  - Paramètres du serveur proxy
  - Exclusion de l'analyse de la mémoire des processus
  - Exclusions globales (points de montage exclus de l'analyse)
  - Zones d'analyse des tâches *ODS, ContainerScan*, *InventoryScan* et *ODFIM*.
- Après l'importation des paramètres, les éléments suivants sont désactivés : Kaspersky Security Network (`UseKSN=No`), le mode Cloud (`CloudMode=No`) et l'intégration MDR (`UseMDR=No`). Gérez les paramètres si vous souhaitez utiliser cette fonctionnalité.

- Après l'importation des paramètres de l'application, les identifiants des tâches internes peuvent changer. Pour gérer les tâches, il est recommandé d'utiliser des noms de tâches.
- En cas d'intégration à Kaspersky Endpoint Detection and Response Expert (cloud), tous les paramètres sont exportés, y compris les paramètres reçus de Kaspersky Endpoint Detection and Response Expert (cloud) :
  - Adresse et port du serveur de télémétrie
  - Adresse et port du serveur de réponse
  - Délai d'attente de la connexion avec les serveurs de réponse
  - Délai d'attente de la réponse du serveur de réponse
  - Délai d'attente de la connexion avec les serveurs de télémétrie
  - Délai d'attente de la réponse du serveur de télémétrie
  - Certificat client du serveur de télémétrie
  - Certificat serveur du serveur de télémétrie
  - Certificat client du serveur de réponse
  - Certificat serveur du serveur de réponse

  Lors de l'importation, les paramètres répertoriés ci-dessus ne sont pas importés sur l'appareil.

Administration de l'application via l'interface graphique

L'administration de l'application via l'interface graphique requiert les droits du rôle Administrateur (admin).

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'interface graphique n'est pas prise en charge.

En **mode standard** de l'application, vous pouvez utiliser l'interface graphique pour :

- Afficher des informations sur l'état de sécurité de l'appareil.
- Configurer les modules de l'application.
  Modules de l'application
  - Protection contre les fichiers malicieux.
  - Gestion du pare-feu.
  - Protection contre le chiffrement.
  - Analyse des disques amovibles.
  - Protection contre les menaces Internet.

- Protection contre les menaces par emails.
- Contrôle des appareils.
- Protection contre les menaces réseau.
- Protection BadUSB.
- Détection comportementale.
- Protection contre les Exploits.
- Contrôle des applications.
- Contrôle Internet.
- Contrôle de l'intégrité du système.

- Analyser les fichiers et les répertoires, y compris en envoyant des fichiers à la Sandbox pour analyse.
- Lancer une mise à jour et annuler les mises à jour des bases de données.
- Activer ou désactiver Kaspersky Security Network pour l'application.
- Demander et obtenir un accès temporaire à un appareil bloqué auprès de l'administrateur du réseau local de l'organisation.
- Gérer les clés de licence de l'application et afficher les informations sur les licences et les clés actuellement utilisées.
- Afficher des informations sur les objets placés dans la sauvegarde.
- Afficher les rapports de l'application.
- Générer des fichiers de trace de l'application.

Icône de l'application dans la zone de notification

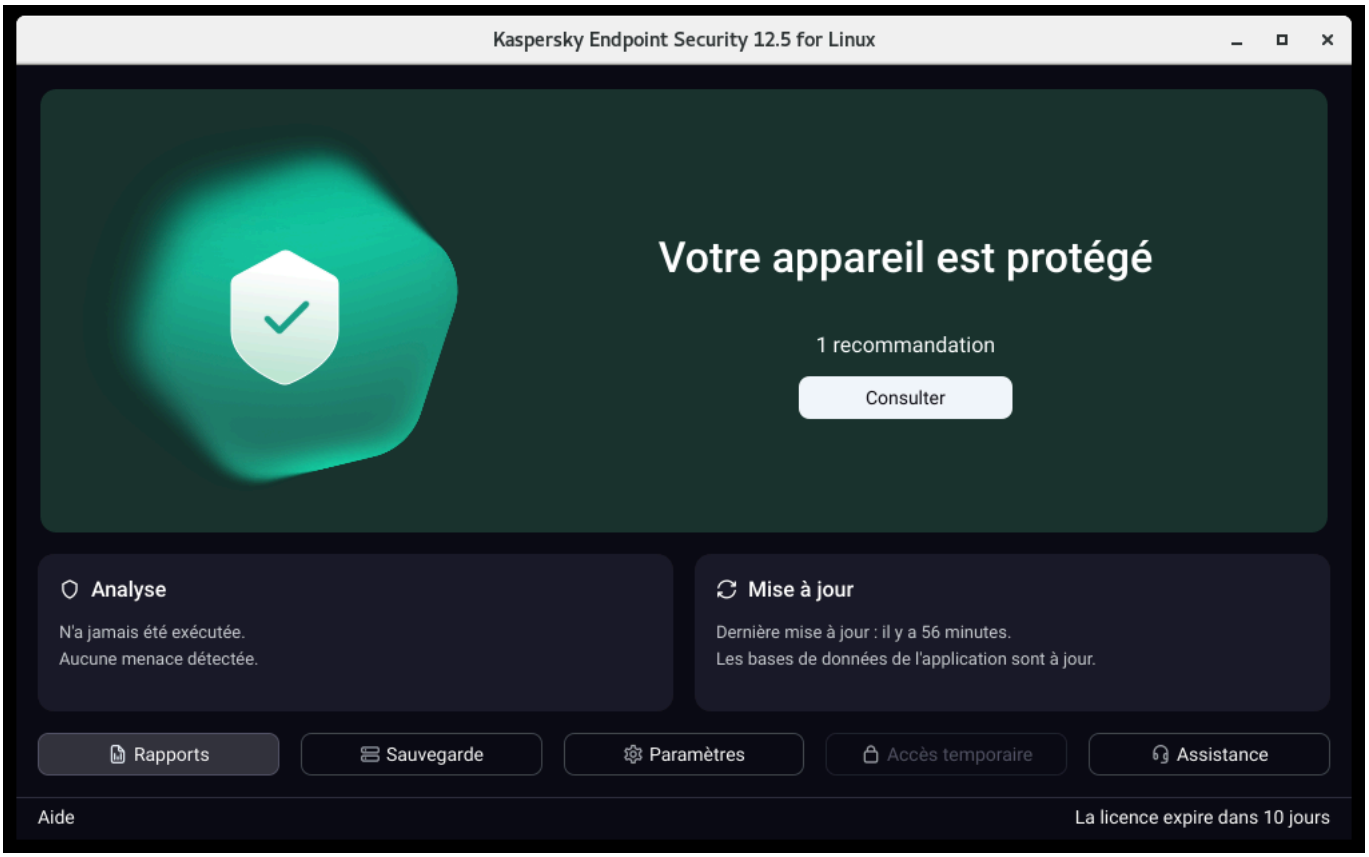
L'icône de l'application Kaspersky Endpoint Security dans la zone de notification de la barre des tâches permet d'accéder au menu contextuel et à la fenêtre principale de l'interface graphique de l'application.

> Sur certains systèmes d'exploitation, l'icône de l'application par défaut peut être manquante après l'installation du paquet d'interface graphique de l'application.

Le menu contextuel de l'icône de l'application reprend les options suivantes :

- **Kaspersky Endpoint Security 12.5 for Linux**. Ouvre la fenêtre principale de l'interface graphique de l'application.
- **Quitter**. Quitte l'interface graphique.

Fenêtre principale de l'interface graphique de l'application



Fenêtre principale de l'application

État de la protection	Informations sur l'état de la protection de l'appareil. Affiché dans la partie supérieure de la fenêtre principale. Vous pouvez cliquer sur le bouton **Afficher** pour ouvrir la fenêtre **Centre de protection**. Cette fenêtre affiche des recommandations sur les actions à effectuer pour corriger les problèmes de protection (le cas échéant).
Analyse	Informations sur l'état de la tâche d'analyse des logiciels malveillants et le nombre de menaces détectées. Vous pouvez cliquer sur cette section pour ouvrir la fenêtre **Analyse**. Dans cette fenêtre, vous pouvez démarrer et arrêter les tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques* et *Analyse du conteneur*, et consulter les rapports relatifs à ces tâches.
Mise à jour.	Informations sur l'état de la tâche de mise à jour des bases de données. Vous pouvez cliquer sur cette section pour ouvrir la fenêtre **Mise à jour**. Dans cette fenêtre, vous pouvez lancer les tâches *Mise à jour* et *Annulation de la mise à jour des bases*, et consulter les rapports relatifs à ces tâches.
Rapports	Affichage des rapports et des statistiques des modules et des tâches.
Sauvegarde	Affichage des détails de l'objet dans Sauvegarde. Que faire si le bouton est inactif
Paramètres	Activation ou désactivation des modules de l'application, configuration de Kaspersky Security Network. Que faire si le bouton est inactif
Accès temporaire	Demande et obtention d'un accès temporaire à un appareil bloqué.
Support technique	Informations relatives à l'application : version actuelle de Kaspersky Endpoint Security, date de publication de la base de données, clé et autres informations. Vous pouvez également consulter les ressources de Kaspersky pour obtenir des informations utiles ou contacter le Support technique.
Durée de validité de la licence	Durée de validité restante de la licence Vous pouvez cliquer sur cette zone pour ouvrir la fenêtre **Licences**. Dans cette fenêtre, vous pouvez consulter des informations détaillées sur votre licence ou visiter le site Internet de Kaspersky pour acheter une nouvelle licence.

Surveillance de l'état de la protection

État de la protection des appareils clients de Kaspersky Security Center

Vous pouvez obtenir des informations sur l'état de la protection d'un appareil dans Kaspersky Security Center à l'aide des états des appareils clients. Pour Kaspersky Security Center, un appareil client est un appareil sur lequel l'Agent d'administration de Kaspersky Security Center est installé.

L'état de l'appareil client peut devenir *Critique* ou *Avertissement* conformément aux règles configurées dans Kaspersky Security Center. Par exemple, l'état peut changer si aucune application de protection n'est installée sur l'appareil, si aucune analyse antivirus n'a été effectuée depuis longtemps, si les bases de l'application sont obsolètes, si la licence a expiré ou si Kaspersky Security Center a reçu l'état de l'appareil depuis une application administrée.

Pour plus d'informations sur les raisons des changements d'état et sur la configuration des conditions d'attribution des états, consultez l'aide de Kaspersky Security Center.

Comment vérifier l'état de la protection d'un appareil dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

4. La fenêtre des propriétés de l'appareil administré s'ouvre ; dans cette fenêtre, sous l'onglet **Général**, sélectionnez la section **Protection**.

Les informations suivantes relatives à l'appareil s'affichent dans la section **Protection** :

- **Visible dans le réseau** : visibilité de l'appareil sélectionné sur le réseau : *Oui* ou *Non*.
- **État de l'appareil** : état de l'appareil client défini sur la base des critères définis par l'administrateur pour l'état de la protection sur l'appareil et l'activité de l'appareil dans le réseau: *OK*, *Critique* ou *Avertissement*.
- **Description de l'état** : raisons du passage de l'appareil à l'état *Critique* ou *Avertissement*.
- **État de la protection** : l'état actuel de la protection contre les menaces de fichiers sur l'appareil sélectionné, par exemple : *En cours d'exécution*, *Arrêté*, *En pause*.
- **Dernière analyse complète** : date et heure de la dernière exécution de la tâche d'analyse complète sur l'appareil sélectionné.

- **Virus détecté** correspond au nombre total d'objets malveillants détectés sur l'appareil sélectionné (compteur des menaces détectées) depuis l'installation de Kaspersky Endpoint Security.

- **Objets dont la désinfection a échoué** : nombre d'objets infectés que l'application Kaspersky Endpoint Security n'a pas pu désinfecter.

Comment vérifier l'état de la protection d'un appareil dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Protection**.

Les informations suivantes relatives à l'appareil s'affichent dans la section **Protection** :

- **État de l'appareil** : état de l'appareil client défini sur la base des critères définis par l'administrateur pour l'état de la protection sur l'appareil et l'activité de l'appareil sur le réseau.

- **Tous les problèmes** : liste complète des problèmes détectés par les applications gérées installées sur l'appareil sélectionné. Chaque problème est associé à un état que l'application vous suggère d'attribuer à un appareil.

- **État de la protection en temps réel** : état actuel de la protection contre les fichiers malicieux sur l'appareil sélectionné, par exemple, *En cours d'exécution* ou *Arrêtée*. Lorsque l'état de protection change, le nouvel état s'affiche dans la fenêtre des propriétés de l'appareil uniquement après la synchronisation de l'appareil avec le serveur d'administration.

- **Dernière tâche d'analyse à la demande** : date et heure auxquelles la dernière recherche d'applications malveillantes a été effectuée sur l'appareil sélectionné.

- **Total de menaces détectées** : nombre total de menaces détectées sur l'appareil sélectionné depuis l'installation de l'application antivirus (première analyse de l'analyse) ou depuis la dernière réinitialisation du compteur de menaces.

  Pour réinitialiser le compteur, cliquez sur le bouton **Mettre à zéro**.

- **Menaces actives** : nombre de fichiers non traités sur l'appareil sélectionné.

Pour plus d'informations sur les états des appareils clients, consultez l'aide de Kaspersky Security Center.

Informations générales sur le fonctionnement de l'application sur l'appareil

Comment consulter les informations générales sur l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Consultez les informations générales sur l'application sous l'onglet **Général**, dans la section **Informations** :

   - **Nom** : nom de l'application.
   - **Version** : numéro de version de l'application.
   - **Installé** : date et heure de l'installation de l'application sur l'appareil.
   - **Dernière mise à jour logicielle** : la date et heure de la dernière mise à jour des modules de l'application Kaspersky Endpoint Security.
   - **Dernière synchronisation** : date et heure de la dernière connexion entre l'appareil et le Serveur d'administration de Kaspersky Security Center.
   - **État en cours** correspond à l'état de l'application sur l'appareil, par exemple *En cours* ou *Arrêté*.
   - Le groupe **Mises à jour installées** contient des informations sur les versions installées des mises à jour pour l'application.
   - Le groupe **Base de données de l'application** contient des informations sur la date et l'heure de publication de la mise à jour des bases de données de l'application, ainsi que sur la date et l'heure de la dernière mise à jour.

7. Consultez les informations sur les modules fonctionnels de l'application sous l'onglet **Général**, dans la section **Modules**. Pour chaque module, l'état (par exemple, *Arrêté, Suspendu, Non installé*) et la version s'affichent.

8. Consultez la liste des événements de l'application sur l'appareil sous l'onglet **Événements**.

Comment consulter les informations générales sur l'application dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.

5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Consultez les informations générales sur la ligne de l'application dans la section **Général**.

   - **Numéro de version** : numéro de version de l'application.
   - **Installé** : date et heure de l'installation de l'application sur l'appareil.
   - **État en cours** correspond à l'état de l'application (service kesl). L'application peut avoir un état tel que *En cours* ou *En pause*.
   - **Dernière mise à jour logicielle** : la date et heure de la dernière mise à jour des modules de l'application Kaspersky Endpoint Security.
   - **Mises à jour installées** : informations sur les versions installées des mises à jour de l'application.
   - **Bases de l'application** : date et heure de publication de la mise à jour des bases de données de l'application.

7. Consultez les informations sur les modules fonctionnels de l'application dans la section **Modules**. Pour chaque module, l'état (par exemple, *Arrêté, Suspendu, Non installé*) et la version s'affichent.

Comment consulter les informations générales sur l'application en ligne de commande

Exécutez la commande :

```
kesl-control --app-info [--json] [--check-permissions]
```

Où :

`--json` : afficher les données au format JSON.

`--check-permissions` affiche les chemins d'accès aux répertoires de l'application dont les autorisations sont configurées de manière incorrecte.

À la suite de l'exécution de la commande, les informations suivantes seront affichées sur la console :

- **Nom**. Le nom de l'application.
- **Version**. Version actuelle de l'application.
- **Stratégie**. Informations indiquant si la stratégie de Kaspersky Security Center est appliquée sur l'appareil.
- Informations détaillées sur la stratégie appliquée sur l'appareil :
  - Nom de la stratégie.
  - La date et l'heure de la dernière application ou mise à jour de la stratégie sur l'appareil.
  - Le groupe d'administration Kaspersky Security Center auquel appartient l'appareil.
  - Liste des profils de stratégie appliqués sur l'appareil (le cas échéant).

> Les informations détaillées sur la stratégie s'affichent si la réception des données étendues de la stratégie de Kaspersky Endpoint Security est activée dans les paramètres de l'Agent d'administration installé sur l'appareil (paramètre **Application peut recevoir des données étendues de la stratégie sur le l'appareil**). Le paramètre est désactivé par défaut. Pour plus d'informations sur les paramètres de l'Agent d'administration, consultez l'aide de Kaspersky Security Center.

- Informations sur la licence sous laquelle l'application est utilisée :
  - **Informations sur la licence de l'application**. Informations sur la licence de l'application ou sur l'état de la clé de licence de l'application.
  - **Date d'expiration de la licence de Kaspersky Endpoint Security**. Date et heure (UTC) de fin de la durée de validité de la licence de l'application.
- Informations sur la licence du module Endpoint Detection and Response Optimum et des modules pour l'intégration aux solutions Kaspersky. Les champs sont affichés si les modules suivants sont activés sur l'appareil protégé :
  - **Informations sur la licence EDR Optimum**. Informations sur la licence sous laquelle le module Kaspersky Endpoint Detection and Response Optimum est activé ou sur l'état de la clé de licence EDR Optimum.
  - **Date de fin de la durée de validité de la licence EDR Optimum**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence KUMA**. Informations sur la licence sous laquelle la fonctionnalité Kaspersky Unified Monitoring and Analysis Platform est utilisée ou sur l'état de la clé de licence KUMA.
  - **Date d'expiration de la licence KUMA**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence MDR**. Informations sur la licence sous laquelle le module Kaspersky Managed Detection and Response est activé ou sur l'état de la clé de licence MDR.
  - **Date d'expiration de la licence MDR**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence EDR Expert (on-premises)**. Informations sur la licence sous laquelle le module Endpoint Detection and Response Expert (on-premises) est activé, ou sur l'état de la clé de licence EDR Expert (on-premises).
  - **Date de fin de la durée de validité de la licence EDR Expert (on-premises)**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence EDR Expert (cloud)**. Informations sur la licence sous laquelle le module Endpoint Detection and Response Expert (on-premises) est activé, ou sur l'état de la clé de licence EDR Expert (cloud).
  - **Date de fin de la durée de validité de la licence EDR Expert (cloud)**. Date et heure (UTC) de fin de la durée de validité de la licence.
- **État de l'abonnement**. État de l'abonnement. Ce champ apparaît si l'application est exécutée sous un abonnement.
- **État du fichier MDR BLOB**. État du fichier BLOB MDR utilisé pour l'intégration avec Kaspersky Managed Detection and Response.
- **Date d'expiration de la licence du fichier MDR BLOB**. Date et heure (UTC) d'expiration de la licence d'utilisation de la fonctionnalité Kaspersky Managed Detection and Response. Ce champ s'affiche si le fichier de configuration BLOB pour l'intégration avec Kaspersky Managed Detection and Response est chargé.
- **État de la sauvegarde**. Informations sur l'état de la sauvegarde.
- **Utilisation de la sauvegarde**. Taille de la sauvegarde.

- **Dernière date d'exécution de la tâche Scan_My_Computer**. Moment auquel la tâche Analyse des logiciels malveillants a été lancée pour la dernière fois.
- **Date de la dernière publication des bases de données**. Date et heure de la dernière publication des bases de l'application.
- **Bases de l'application chargées**. Informations indiquant si les bases de données de l'application sont chargées.
- **État du module de noyau mis à jour**. Informations sur l'état du module de noyau mis à jour.
- **Utilisation de Kaspersky Security Network**. Informations sur l'utilisation de Kaspersky Security Network : `Mode étendu de KSN`, `Mode KSN de base` ou `Désactivé`.
- **Mode Light Agent**. Informations sur l'utilisation de l'application en mode Light Agent. Si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent, cette ligne n'est pas affichée.
- **Mode Endpoint Detection and Response Agent**. Informations sur l'utilisation de l'application en mode EDR Agent. Si l'application est utilisée en mode standard ou en mode Light Agent, cette ligne n'est pas affichée.
- **Infrastructure de Kaspersky Security Network**. Informations sur la solution d'infrastructure utilisée pour travailler avec les bases de données de réputation de Kaspersky : `Kaspersky Security Network` ou `Kaspersky Private Security Network`.
- **Intégration avec Kaspersky Managed Detection and Response**. État de l'intégration avec Kaspersky Managed Detection and Response.
- **Intégration avec Kaspersky Endpoint Detection and Response Optimum**. État d'intégration avec Kaspersky Endpoint Detection and Response Optimum.
- **Protection contre les fichiers malicieux**. État de la protection contre les menaces de fichiers en temps réel.
- **Surveillance du conteneur**. État de l'analyse du conteneur en temps réel.
- **Contrôle de l'intégrité du système**. État du module Contrôle de l'intégrité du système.
- **Gestion du pare-feu**. État du module Gestion du Firewall.
- **Protection contre le chiffrement**. État du module Protection contre le chiffrement.
- **Protection contre les menaces Internet**. État du module Protection contre les menaces Internet.
- **Contrôle des appareils**. État du module Contrôle des appareils.
- **Analyse des disques amovibles**. État du module Analyse des disques amovibles.
- **Protection BadUSB**. État du module Protection BadUSB.
- **Protection contre les menaces réseau**. État du module Protection contre les menaces réseau.
- **Détection comportementale**. État du module Détection comportementale.
- **Contrôle des applications**. État du module Contrôle des applications.
- **Contrôle Internet**. État du module Contrôle Internet.

- **Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)**. État de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA).

- **Intégration de Kaspersky Endpoint Detection and Response Expert (cloud)**. État de l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).

- **Intégration avec Sandbox**. État de l'intégration avec Sandbox.

- **Intégration avec Kaspersky Unified Monitoring and Analysis Platform**. État d'intégration avec Kaspersky Unified Monitoring and Analysis Platform.

- **Intégration avec Kaspersky Network Detection and Response (KATA)** État de l'intégration avec Kaspersky Network Detection and Response (KATA).

- **Protection contre les menaces par emails**. État du module Protection contre les menaces par emails.

- **Actions après la mise à jour**. Les actions relatives à la mise à jour de l'application et aux actions qu'un utilisateur doit effectuer.

- **L'application est instable**. Informations sur la création de fichiers de vidage en cas de plantage de l'application. Ce champ s'affiche si des fichiers sont détectés dans le répertoire de vidage.

- **État de l'application**. Informations sur l'état de la connexion de l'Agent d'administration et sur les autorisations pour les répertoires système :

  - *OK*. L'Agent d'administration est connecté, les autorisations pour les répertoires système sont correctement configurées.

  - *Critique. Aucune connexion à l'Agent d'administration*.

  - *Critique. Les autorisations des répertoires système sont mal configurées*.

  - *Critique. Aucune connexion à l'Agent d'administration. Les autorisations pour les répertoires système sont mal configurées*.

Comment consulter les informations générales sur l'application dans l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Dans la partie inférieure de la fenêtre principale, cliquez sur le bouton **Assistance**.

   La fenêtre **Support** s'ouvre.

3. Consultez les informations générales sur l'appareil et l'application installée :

   - Version de l'application.

   - **Clé de licence** : clé de licence de base active ajoutée à l'application, ou informations sur l'absence de clé. Un clic sur le lien dans ce champ ouvre la fenêtre **Licences**, qui affiche des informations détaillées sur la licence.

   - **État de la clé** : informations sur l'état de la clé de licence de base active ou informations sur l'absence de clé.

   - **Date de publication de la base de données** : état et date de publication des bases de données de l'application.

- **Système d'exploitation** : informations sur le système d'exploitation de l'appareil ;
- **Administration de l'application** : informations indiquant si l'appareil est sous gestion d'une stratégie.

Si le paramètre **L'application peut recevoir des données étendues de la stratégie sur le l'appareil** est activé dans la stratégie de l'Agent d'administration, la fenêtre affiche également les informations suivantes sur la stratégie appliquée sur l'appareil sur lequel l'application est installée.

- **Nom de la stratégie** : nom de la stratégie sous laquelle fonctionne l'appareil avec l'application installée.
- **Date d'application de la stratégie** : date et heure de la dernière application ou mise à jour de la stratégie sur l'appareil sur lequel l'application est installée.
- **Groupe d'administration** : nom du groupe d'administration qui inclut l'appareil sur lequel l'application est installée et exécutée sous la gestion des stratégies.
- **Profils actifs de la stratégie** : liste des profils actifs de la stratégie appliqués sur l'appareil (le cas échéant).

Statistiques de l'application

Vous pouvez consulter les statistiques relatives aux fichiers analysés et aux processus démarrés le plus fréquemment.

Vous pouvez configurer le mode de calcul et d'affichage des statistiques par l'application dans le fichier de configuration kesl.ini, dans la section `[ScannerImpactStats]`.

Comment consulter les statistiques d'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.
5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.
6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Statistiques → Statistiques de l'analyse**.

7. Consultez les statistiques de l'application dans la fenêtre **Statistiques d'analyse** :

   - La section **Fichiers les plus fréquemment analysés (Protection contre les fichiers malicieux)** affiche les chemins d'accès aux fichiers que le module Protection contre les fichiers malicieux analyse le plus fréquemment et le nombre de fois que le module accède à ces fichiers. Les fichiers sont affichés par ordre décroissant du nombre de fois où ils ont été consultés.

   - Le groupe **Applications les plus fréquemment analysées** affiche les chemins d'accès aux processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, ainsi que le nombre de ces lancements. Les chemins d'exécution des processus sont affichés par ordre décroissant du nombre d'exécutions.

   Vous pouvez cliquer sur les boutons **Exporter** situés dans la partie supérieure de chaque zone pour exporter les statistiques correspondantes dans un fichier texte.

Comment consulter les statistiques d'analyse dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.

5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.

6. Dans la fenêtre qui s'ouvre, sélectionnez la section **Statistiques** → **Statistiques de l'analyse**.

7. Consultez les statistiques de l'application :

   - La section **Fichiers les plus fréquemment analysés (Protection contre les fichiers malicieux)** affiche les chemins d'accès aux fichiers que le module Protection contre les fichiers malicieux analyse le plus fréquemment et le nombre de fois que le module accède à ces fichiers. Les fichiers sont affichés par ordre décroissant du nombre de fois où ils ont été consultés.

   - Le groupe **Applications les plus fréquemment analysées** affiche les chemins d'accès aux processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, ainsi que le nombre de ces lancements. Les chemins d'exécution des processus sont affichés par ordre décroissant du nombre d'exécutions.

   Vous pouvez cliquer sur les boutons **Exporter** situés sous chaque zone pour exporter les statistiques correspondantes dans un fichier texte.

Comment consulter les statistiques d'analyse en ligne de commande

Exécutez la commande :

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

Où :

- `--files` : statistiques sur les fichiers que le module Protection contre les fichiers malicieux analyse le plus souvent et le nombre de fois où le module accède à ces fichiers ;
- `--processes` : statistiques sur les processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, et le nombre de ces lancements ;

  L'exclusion de processus de l'analyse par le module Détection comportementale ne les supprime pas des statistiques, mais améliore les performances de Kaspersky Endpoint Security.

Si vous ne spécifiez pas de clés, l'application affichera trois listes : des statistiques sur les fichiers les plus fréquemment analysés, des statistiques sur les processus les plus fréquemment lancés et une liste des points de montage détectés sur l'appareil.

Sous CentOS 5.2, 5.4, 6.4 et 6.6, les statistiques relatives aux fichiers fréquemment analysés ne sont pas collectées.

Points de montage détectés

Vous pouvez consulter la liste des points de montage détectés sur l'appareil. La liste affiche des informations indiquant si le point de montage a été ajouté aux exclusions de l'analyse.

Comment consulter la liste des points de montage dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Statistiques → Points de montage**.

   La fenêtre **Points de montage** s'ouvre.

7. Consultez les informations sur les points de montage dans le tableau :

   - **Chemin du point de montage** : chemin d'accès au point de montage détecté sur l'appareil.
   - **Espace de noms** : informations sur la détection du point de montage dans l'espace de noms.
   - **Exclu** : informations indiquant si le point de montage est ajouté aux exclusions d'analyse.

   Les chemins d'accès aux points de montage sont triés comme suit :

   - points de montage statiques, système, de service et autres
   - paquets snap montés et points de montage dans leurs espaces de noms
   - Points de montage créés par le système de gestion des conteneurs Docker

   En cliquant sur le bouton **Exporter** situé dans la partie supérieure de la fenêtre, au-dessus de la liste, vous pouvez exporter la liste des points de montage dans un fichier texte. Le fichier contient une liste de chemins d'accès aux points de montage, ainsi que les étiquettes **[Espace de noms]** et **[Exclu]**.

Comment consulter la liste des points de montage dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.
6. Cette action ouvre la fenêtre des propriétés de l'application ; dans cette fenêtre, sélectionnez la section **Statistiques → Points de montage**.
7. Consultez les informations sur les points de montage dans le tableau **Liste des points de montage** :

   - **Chemin du point de montage** : chemin d'accès au point de montage détecté sur l'appareil.
   - **Espace de noms** : informations sur la détection du point de montage dans l'espace de noms.
   - **Exclu** : informations indiquant si le point de montage est ajouté aux exclusions d'analyse.

   Les chemins d'accès aux points de montage sont triés comme suit :

   - points de montage statiques, système, de service et autres
   - paquets snap montés et points de montage dans leurs espaces de noms
   - Points de montage créés par le système de gestion des conteneurs Docker

À l'aide du bouton **Exporter** situé sous la liste, vous pouvez exporter la liste des points de montage vers un fichier au format texte. Le fichier contient une liste de chemins d'accès aux points de montage, ainsi que les étiquettes `[Espace de noms]` et `[Exclu]`.

Comment consulter la liste des points de montage en ligne de commande

Exécutez la commande :

```
kesl-control [-S] --get-statistic --mountpoints
```

La sortie affiche les informations suivantes :

- `[excluded]` : indique si le point de montage a été ajouté aux exclusions d'analyse.
- `[namespace]` : informations sur la détection du point de montage dans l'espace de noms ;
- chemin d'accès au point de montage détecté sur l'appareil.

Les chemins d'accès aux points de montage sont triés comme suit :

- points de montage statiques, système, de service et autres
- paquets snap montés et points de montage dans leurs espaces de noms
- Points de montage créés par le système de gestion des conteneurs Docker

Liste des fonctionnalités et des technologies

En ligne de commande, vous pouvez consulter la liste des fonctionnalités de l'application avec des informations sur leur état (utilisées ou non) et les technologies Linux à l'aide desquelles ces fonctionnalités de l'application sont implémentées.

Consulter la liste des fonctionnalités et des technologies

```
kesl-control --supported-tech-info
```

À la suite de l'exécution de la commande, les informations suivantes seront affichées sur la console :

Interception des opérations sur les fichiers :

État : utilisé ou non utilisé

Technologies : fanotify, module de noyau de la Protection contre les fichiers malicieux, module de noyau mis à jour.

Interception du lancement des processus :

État : utilisé ou non utilisé

Technologies : eBPF, kprobe, netlink, undefined, module de noyau mis à jour.

Analyse du trafic réseau :

État : utilisé ou non utilisé

Technologies : eBPF, iptables, undefined.

Utilitaire iptables :

État : utilisé ou non utilisé

Technologies : ipv6, undefined, timeout, prise en charge de plusieurs étiquettes dans les règles.

Isolation du réseau :

État : utilisé ou non utilisé

Technologies : eBPF, iptables, undefined.

Protection contre les Exploits :

État : utilisé ou non utilisé

Technologies : undefined, module de noyau mis à jour.

États de la protection en temps réel

L'état de la Protection en temps réel de l'ordinateur détermine l'état du module Protection contre les fichiers malicieux. La Protection contre les fichiers malicieux offre un niveau minimal de sécurité à l'ordinateur. Le module est lancé avec Kaspersky Endpoint Security et analyse les fichiers en temps réel.

États de la protection en temps réel

État dans Kaspersky Security Center	État dans la ligne de commande	Description
En cours d'exécution	Démarré	La tâche Protection contre les fichiers malicieux est lancée et en cours d'exécution.
Lancement en cours	En cours de démarrage ou Reprise	Essayez de lancer la tâche Protection contre les fichiers malicieux. Attendez le lancement de la tâche.
Arrêté(e)	Arrêté ou En cours d'arrêt	La tâche Protection contre les fichiers malicieux a été arrêtée manuellement. Lancez la tâche dans Kaspersky Security Center ou localement sur l'ordinateur. Si l'application est installée en mode Light Agent, l'appareil obtient cet état en l'absence de connexion à la SVM.
Suspendu(e)	En pause ou Suspendu	La tâche Protection contre les fichiers malicieux a été suspendue manuellement. Lancez la tâche dans Kaspersky Security Center ou localement sur l'ordinateur.
Non défini		L'application est installée en mode EDR Agent. Le module Protection contre les fichiers malicieux fonctionne en mode Inform.
Inconnu		Erreur inconnue.

Comment connaître l'état de la Protection en temps réel de l'ordinateur

Vous pouvez connaître l'état de la Protection en temps réel de l'ordinateur dans une console Kaspersky Security Center, dans la liste des appareils administrés, ou localement sur votre ordinateur.

Comment connaître l'état de la Protection en temps réel de l'ordinateur dans Web Console

Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

L'état actuel de la protection s'affiche dans la liste des appareils, dans la colonne **État de protection en temps réel ;**. Si la colonne **État de protection en temps réel ;** est absente, gérez les paramètres des colonnes (⚙).

Comment connaître l'état de la Protection en temps réel de l'ordinateur dans la ligne de commande

Exécutez la commande :

```
kesl-control --get-task-state 1
```

Par conséquent, Kaspersky Endpoint Security affiche les informations sur le fonctionnement de la Protection contre les fichiers malicieux au format suivant :

Nom: File_Threat_Protection	
ID	: 1
Type	: OAS
État	: <protection status>

Que faire si l'état de la Protection en temps réel de l'ordinateur n'est pas En cours d'exécution

1. Assurez-vous que la Protection contre les fichiers malicieux est activée dans les propriétés de la stratégie.
2. Assurez-vous que l'application est activée.
3. Essayez de lancer la tâche Protection contre les fichiers malicieux :

   Comment lancer la tâche Protection contre les fichiers malicieux dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

      La liste des appareils administrés s'affiche.
   2. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.
   3. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, accédez à l'onglet **Tâches**.

      Cette action ouvre la liste de toutes les tâches sur l'appareil.
   4. Sélectionnez la tâche **Protection contre les fichiers malicieux** et cliquez sur le bouton **Lancer**.

Comment lancer la tâche Protection contre les fichiers malicieux dans la ligne de commande

Exécutez la commande :

```
kesl-control --start-task 1
```

Événements et rapports

Différents *événements* se produisent pendant le fonctionnement de l'application. Ils peuvent avoir un caractère informatif ou revêtir une importance plus grande. Ainsi, l'application peut utiliser les événements pour signaler la réussite de la mise à jour des bases de données de l'application ou signaler une erreur dans le fonctionnement d'un module qu'il faudra rectifier.

Kaspersky Endpoint Security vous permet de saisir des informations sur les événements survenus pendant le fonctionnement de l'application dans les journaux suivants :

- Journal des événements de l'application. Par défaut, l'application stocke les informations sur les événements dans les fichiers de base de données du journal des événements situés dans le répertoire /var/opt/kaspersky/kesl/private/storage. Vous pouvez configurer les paramètres du journal des événements de l'application à partir de la ligne de commande.

- Journal du système d'exploitation (syslog). Par défaut, le journal du système d'exploitation n'est pas utilisé. Vous pouvez activer l'enregistrement des événements dans ce journal.

Les privilèges root sont requis pour accéder au journal des événements de l'application et au journal du système d'exploitation.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les informations sur les événements peuvent être transmises au Serveur d'administration de Kaspersky Security Center. Certains événements ont des règles d'agrégation. Si de nombreux événements du même type sont générés pendant une courte période pendant le fonctionnement de l'application, l'application passe en mode d'agrégation d'événements et envoie un événement agrégé avec une description des paramètres de ces événements à Kaspersky Security Center. Différentes règles d'agrégation peuvent être utilisées pour différents événements. Pour plus d'informations sur les événements, consultez l'aide de Kaspersky Security Center.

Vous pouvez recevoir des informations sur les événements de l'application des manières suivantes :

- Dans la Console d'administration et dans Web Console.

- Dans la ligne de commande.

- Lors de l'utilisation de l'interface utilisateur graphique de l'application : dans les notifications contextuelles, si l'affichage des notifications est activé dans les propriétés de la stratégie ou dans les paramètres généraux de l'application

En fonction des événements qui se produisent pendant l'exécution de l'application, vous pouvez générer divers *rapports*. Les rapports enregistrent des informations sur le fonctionnement de chaque module de l'application Kaspersky Endpoint Security, les résultats de chaque tâche et le fonctionnement de l'ensemble de l'application dans son ensemble.

Vous pouvez consulter les rapports d'une des manières suivantes :

- Les rapports de Kaspersky Security Center sont disponibles dans la Console d'administration et dans Web Console. Avec leur aide, vous pouvez, par exemple, obtenir des informations sur les fichiers infectés, l'utilisation des clés et des bases de données de l'application. Pour en savoir plus sur l'utilisation des rapports de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

- L'interface utilisateur graphique de Kaspersky Endpoint Security affiche les rapports de l'application, de ses modules et de ses tâches.

Contenu des rapports et des événements

Les rapports et les événements peuvent contenir les données personnelles suivantes :

- noms et identifiants des utilisateurs dans le système d'exploitation ;
- chemins d'accès aux fichiers utilisateur ;
- adresses IP des appareils distants analysés par le module Protection contre le chiffrement ;
- adresses IP des expéditeurs et des destinataires des paquets réseau vérifiés par le module Gestion du pare-feu ;
- adresses Internet des sources de mises à jour ;
- valeurs des paramètres généraux de l'application ;
- noms et paramètres des tâches de la ligne de commande ;
- adresses Internet malveillantes, de phishing, publicitaires et adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager vos appareils ou vos données ;
- noms des conteneurs et des images ;
- chemins d'accès aux conteneurs et images ;
- noms et identifiants des appareils ;
- noms des catégories des applications ;
- adresses Internet des référentiels ;
- noms de fichiers, chemins d'accès aux fichiers et sommes de hachage des fichiers exécutables des applications.

Règles d'échappement des caractères dans les chemins de fichiers

Certains événements peuvent contenir des chemins d'accès aux fichiers. Lors de l'affichage, le chemin d'accès au fichier est traité comme une chaîne codée en UTF-8. Si l'un des octets du chemin n'est pas conforme aux règles de codage UTF-8, il est alors remplacé par le caractère ?. Une séquence de quatre octets codant le code des caractères en dehors de la plage Unicode (supérieure à 0x10FFFF) est également remplacée par le caractère ?. Les caractères spéciaux sont échappés (remplacés) d'une manière spécifique.

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lors de l'affichage à l'aide de la commande `kesl-control -E --query` :

- les caractères '\a', '\b', '\t', '\n', ' \v', '\f', '\r' sont remplacés par deux caractères comme suit :

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- tous les autres caractères spéciaux sont affichés inchangés.

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lors de l'affichage à l'aide de la commande `kesl-control -E --query --json` :

- les caractères '\b', '\f', '\n', '\r', '\t', '"', '\\' sont échappés, selon le format JSON, comme suit :

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- tous les autres caractères spéciaux sont échappés conformément aux règles générales d'échappement des caractères spéciaux pour le format JSON ('\a' -> '\u0007').

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lorsqu'ils sont envoyés à syslog :

- les caractères '\b', '\f', '\n', '\r', '\t', '"', '\\' sont échappés, selon le format JSON, comme suit :

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- tous les autres caractères spéciaux sont échappés conformément aux règles générales d'échappement des caractères spéciaux pour le format JSON ('\a' -> '\u0007').

La première barre oblique de la séquence lors de la description des règles est un caractère d'échappement.

Exemples :
`'\a'` est un caractère (administrateur) ;

`'\\a'` correspond à deux caractères (barre oblique inverse + caractère « a »).

`'\\'` est un caractère (barre oblique inverse), `'\\\\'` ce sont deux caractères (barre oblique inverse + abarre oblique inverse).

Configuration d'enregistrement des événements dans le journal du système d'exploitation

Les événements survenus lors du fonctionnement de l'application Kaspersky Endpoint Security peuvent être enregistrés dans le journal du système d'exploitation (syslog). Vous pouvez activer ou désactiver l'enregistrement des événements dans ce journal à l'aide de Web Console, de la Console d'administration ou de la ligne de commande.

Par défaut, la journalisation des événements dans le journal du système d'exploitation est désactivée.

Si Kaspersky Endpoint Security fonctionne en mode standard ou en mode EDR Agent et est administré par une stratégie dans Kaspersky Security Center, les informations relatives à l'ajout et à la suppression des clés de licence, ainsi qu'à l'expiration de la licence, sont consignées par défaut dans le journal du système d'exploitation. Vous pouvez sélectionner les événements qui seront écrits dans le journal du système d'exploitation dans les propriétés de la stratégie sous laquelle l'application s'exécute.

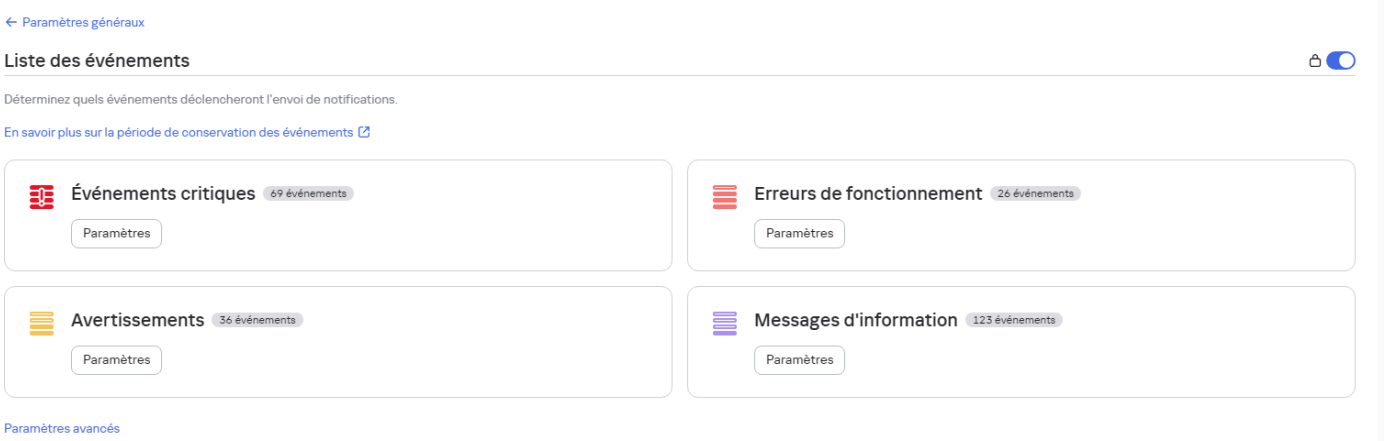
Comment configurer la journalisation des événements dans syslog dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security for Linux.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Accédez à l'onglet **Paramètres de l'application**.
4. Sélectionnez **Paramètres généraux** → **Paramètres des événements**.

   Les types d'événements sont affichés regroupés par niveau de gravité.
5. Cliquez sur le bouton **Paramètres** dans le bloc portant le nom du niveau de gravité correspondant à l'événement pour lequel vous souhaitez configurer la journalisation dans le journal du système d'exploitation.

   Une fenêtre contenant la liste de tous les événements du niveau de gravité sélectionné s'ouvre. Vous pouvez activer ou désactiver séparément la journalisation dans le journal du système d'exploitation pour chaque événement.
6. Dans la colonne **Événements**, cliquez sur le nom de l'événement pour lequel vous souhaitez configurer la journalisation dans le journal du système d'exploitation.
7. Accédez à l'onglet **Notifications**.
8. Cochez ou décochez la case **Enregistrer dans le journal des événements du système d'exploitation**.



Paramètres de notification des événements

Comment configurer la journalisation des événements dans syslog dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

4. Accédez à la section **Paramètres généraux → Interface**.

5. Sous **Notifications**, cliquez sur **Configurer**.

   La fenêtre **Paramètres de notification** s'ouvre.

6. Utilisez les cases à cocher pour sélectionner les événements que l'application enregistre dans le journal du système d'exploitation.

   Vous pouvez également sélectionner tous les événements d'un niveau de gravité donné :

   - *Les événements critiques* sont des événements qui constituent une menace sérieuse pour la sécurité des appareils (détection d'objets malveillants, vulnérabilités, problèmes de fonctionnement des applications). Un événement critique nécessite votre attention immédiate. Il est recommandé de ne pas désactiver les notifications concernant les événements critiques.

   - *Les erreurs de fonctionnement* sont des événements qui se produisent lorsqu'une application dysfonctionne (erreur de traitement, erreur de configuration de tâche). Ces événements ne représentent pas une menace directe pour la sécurité de l'appareil, mais ils nécessitent votre intervention pour que l'application fonctionne correctement.

   - *Les avertissements* sont des événements qui ne nécessitent pas d'intervention immédiate de votre part, mais qui peuvent représenter une menace pour la sécurité de votre appareil.

   - *Les messages d'information* sont des événements informatifs.

Comment configurer la journalisation des événements dans syslog en ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver l'enregistrement des événements dans le journal du système d'exploitation à l'aide de l'option `UseSyslog` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Activer ou désactiver la journalisation des événements dans syslog

```
kesl-control --set-app-settings UseSyslog=<Yes|No>
```

Où :

- `Yes` : active l'enregistrement de tous les événements dans syslog.
- `No` (valeur par défaut) : désactiver l'enregistrement des événements dans syslog.

Configuration des paramètres du journal des événements de l'application

Par défaut, les informations sur les événements sont stockées dans le journal des événements de l'application situé sur l'appareil.

La base de données du journal des événements contient les fichiers suivants :

- plusieurs fichiers avec des événements. Le nombre de fichiers dépend du nombre actuel d'événements dans le journal des événements et du nombre maximal d'événements que l'application stockera (défini dans le paramètre `MaxEventsNumber`).

  Le nom du fichier d'événements contient le numéro de série de sa création (par exemple, events.db.0001). Les fichiers sont créés au fur et à mesure qu'ils sont remplis. Si tous les fichiers d'événements, à l'exception du fichier le plus ancien, ont un nombre maximal d'événements égal à la valeur spécifiée du paramètre `MaxEventsNumber`, le fichier le plus ancien est supprimé. De cette façon, l'application peut stocker plus d'événements que défini dans le paramètre.

- le fichier principal de la base de données pour la gestion des fichiers des événements, qui stocke des informations sur les fichiers journaux des événements. Ce fichier ne peut pas être supprimé.

À partir de la ligne de commande, vous pouvez gérer les paramètres suivants du journal des événements de l'application à l'aide des paramètres généraux de l'application :

- Modifier le chemin d'accès au fichier principal de la base de données du journal des événements à l'aide du paramètre `EventsStoragePath`. Valeur par défaut : /var/opt/kaspersky/kesl/private/storage/events.db.
- Définissez le nombre maximum d'événements que l'application stockera à l'aide du paramètre `MaxEventsNumber`. Valeur par défaut : 500 000.

Vous pouvez consulter les paramètres actuels dans les paramètres généraux de l'application sur la ligne de commande ou dans le fichier de configuration.

Afficher les valeurs actuelles des paramètres généraux de l'application dans la console

```
kesl-control --get-app-settings [--json]
```

Où `--json` est spécifié pour afficher les paramètres au format JSON.

```
Afficher les valeurs actuelles des paramètres généraux de l'application dans un fichier de configuration

kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Où `--file <path to configuration file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez afficher les paramètres généraux de l'application. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

```
Modification des paramètres des événements à l'aide des options de ligne de commande

kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Où <nom du paramètre>=<valeur du paramètre> correspond au nom et à la valeur d'un des paramètres.

```
Modification des paramètres des événements à l'aide du fichier de configuration

kesl-control --set-app-settings --file <path to configuration file> [--json]
```

Où :

- `--file <path to configuration file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux de l'application. Si vous supprimez un paramètre dans le fichier de configuration, la valeur par défaut de ce paramètre sera affichée après l'exécution de la commande.

- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si l'option --json n'est pas spécifiée, l'application tente d'importer depuis un fichier INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres généraux spécifiées dans le fichier seront importées dans l'application.

Affichage des événements de l'application

Affichage de tous les événements de l'application Kaspersky Endpoint Security dans Kaspersky Security Center

Les événements qui surviennent lors du fonctionnement de l'application Kaspersky Endpoint Security sont classés par niveau d'importance selon les types suivants :

- *Les événements critiques* sont des événements qui constituent une menace sérieuse pour la sécurité des appareils (détection d'objets malveillants, vulnérabilités, problèmes de fonctionnement des applications). Un événement critique nécessite votre attention immédiate. Il est recommandé de ne pas désactiver les notifications concernant les événements critiques.

- *Les erreurs de fonctionnement* sont des événements qui se produisent lorsqu'une application dysfonctionne (erreur de traitement, erreur de configuration de tâche). Ces événements ne représentent pas une menace directe pour la sécurité de l'appareil, mais ils nécessitent votre intervention pour que l'application fonctionne correctement.

- *Les avertissements* sont des événements qui ne nécessitent pas d'intervention immédiate de votre part, mais qui peuvent représenter une menace pour la sécurité de votre appareil.

- *Les messages d'information* sont des événements informatifs.

Une liste de tous les événements liés au fonctionnement de l'application Kaspersky Endpoint Security est affichée dans Web Console et dans la Console d'administration.

Comment afficher la liste de tous les événements dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Accédez à l'onglet **Configuration des événements**.

   La liste de tous les événements, filtrée par niveau de gravité, s'affiche.

4. Utilisez le menu de gauche pour afficher tous les événements d'autres niveaux de gravité.

Comment afficher la liste de tous les événements dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

4. Accédez à la section **Paramètres généraux** → **Paramètres de notification**.

5. Sous **Notifications**, cliquez sur **Configurer**.

   La fenêtre **Paramètres de notification** s'ouvre.

Vous pouvez configurer des notifications d'événements. Grâce aux notifications, vous pouvez recevoir des informations en temps opportun sur les événements de l'application. Vous pouvez configurer l'exécution du script à la réception d'un événement depuis l'application ou à la réception d'une notification par email sur les événements. Pour plus d'informations sur l'utilisation des notifications de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Affichage des événements dans l'interface graphique de l'application

Dans l'interface graphique de l'application, les informations relatives aux événements s'affichent par défaut sous forme de notifications contextuelles.

Comment configurer les notifications contextuelles dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security for Linux.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Accédez à l'onglet **Paramètres de l'application**.
4. Sélectionnez **Paramètres généraux** → **Paramètres des événements**.
5. Cliquez sur le lien **Paramètres complémentaires**.

   La fenêtre **Paramètres avancés** s'ouvre.
6. Cochez ou décochez la case **Afficher les notifications contextuelles dans l'interface utilisateur graphique**. La case est cochée par défaut.
7. Enregistrez vos modifications.

Comment configurer les notifications contextuelles dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.
4. Accédez à la section **Paramètres généraux** → **Paramètres de notification**.
5. Cochez ou décochez la case **Afficher les notifications contextuelles dans l'interface utilisateur graphique**. La case est cochée par défaut.

Comment configurer les notifications contextuelles en ligne de commande

À partir de la ligne de commande, vous pouvez basculer l'affichage des notifications contextuelles dans l'interface graphique en utilisant le paramètre `ShowPopUpNotifications` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

```
Active l'affichage des notifications contextuelles dans l'interface graphique

kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

Où :

- `Yes` (par défaut) : afficher les notifications contextuelles dans l'interface utilisateur graphique.
- `No` : ne pas afficher les notifications contextuelles dans l'interface utilisateur graphique.

Affichage des événements en cours de l'application Kaspersky Endpoint Security en ligne de commande

En ligne de commande, vous pouvez afficher des informations sur tous les événements en cours dans l'application ou sur les événements associés à la tâche indiquée. À l'aide d'un filtre vous pouvez également afficher certains événements en cours, par exemple, des événements d'un type spécifié.

```
Afficher dans la console des informations sur tous les événements en cours de l'application

kesl-control -W
```

La commande reprend le nom de l'événement et les informations supplémentaires sur l'événement.

```
Exécuter la tâche et afficher dans la console des informations sur les événements en cours qui lui sont associés

kesl-control --start-task <task ID|name> -W
```

où `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

Cette commande lance la tâche portant l'ID ou le nom indiqué et active l'affichage des événements en cours associés à la tâche. Les événements sont affichés dès qu'ils sont générés par cette tâche.

```
Exemple de lancement de la tâche avec ID=1 et d'activation de l'affichage de ses événements

kesl-control --start-task 1 -W
```

```
Afficher dans la console des informations sur les événements en cours qui correspondent aux conditions du filtre

kesl-control -W --query "<filter conditions>"
```

où `<filter conditions>` désigne une ou plusieurs expressions logiques au format `<field> <comparison operation> '<value>'`, combinées par l'opérateur logique `and`.

```
Exemple de sortie de l'événement TaskStateChanged

kesl-control -W --query "EventType == 'TaskStateChanged'"
```

```
Exemple de sortie de l'événement TaskSettingsChanged initié par l'utilisateur 'User'

kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Affichage des événements du journal des événements de l'application

En ligne de commande, vous pouvez afficher dans la console ou enregistrer dans un fichier des informations sur les événements du journal des événements de l'application. Pour afficher un sous-ensemble d'événements, utilisez le filtrage.

Afficher des informations sur tous les événements du journal des événements de l'application dans la console

```
kesl-control -E --query [--db <database file>]
```

où `<database file>` est le chemin complet du fichier de base de données du journal des événements à partir duquel afficher les événements.

Par défaut, l'application stocke les informations relatives aux événements dans la base de données `/var/opt/kaspersky/kesl/private/storage/events.db`. L'emplacement de la base de données est déterminé par le paramètre général de l'application `EventsStoragePath`.

Si le journal des événements se trouve dans la base de données par défaut, utilisez la commande suivante pour afficher les événements dans la console :

```
kesl-control -E
```

Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés. Par défaut, l'application stocke jusqu'à 500 000 événements. Le nombre maximal d'événements stockés par l'application est déterminé par le paramètre général de l'application `MaxEventsNumber`.

Afficher dans la console des informations sur les événements du journal des événements de l'application qui répondent à certains critères

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

où :

- `<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête.
- `<number>` correspond au nombre des événements les plus récents de la sélection (c'est-à-dire au nombre d'enregistrements comptés à partir de la fin de la sélection) que vous souhaitez afficher.
- `--json` – afficher les événements au format JSON.
- `--reverse` : afficher les événements dans l'ordre inverse (de l'événement le plus récent en haut au plus ancien en bas).

Enregistrer dans un fichier des informations sur tous les événements du journal des événements de l'application

```
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

où `--file <path to file>` est le chemin complet du fichier dans lequel vous souhaitez enregistrer les événements.

Articles utiles

Que faire en cas de faux positifs

Consulter les rapports

La consultation des rapports est disponible uniquement dans l'interface graphique de l'application.

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, à l'exécution de chaque tâche d'analyse, de la tâche de mise à jour et de la tâche de vérification de l'intégrité, ainsi qu'au fonctionnement de l'application dans son ensemble, sont consignées dans des *rapports*.

Les rapports prévoient les gravités suivantes pour les événement :

- *Critique* : événements critiques auxquels vous devez prêter attention, car ils indiquent un problème avec l'application ou une vulnérabilité dans la protection de l'appareil.
- *Élevé*.
- *Moyen*.
- *Faible*.
- *Informatif*.
- *Erreur*.

Les rapports suivants sont disponibles dans l'application :

- **Statistiques**. Statistiques de la Protection contre les fichiers malicieux et des tâches d'analyse. Vous pouvez mettre à jour le rapport affiché en cliquant sur le bouton **Mettre à jour**.
- **Audit du système**. Informations sur les événements qui se produisent lors du fonctionnement de l'application et lors de l'interaction de l'utilisateur avec l'application.
- **Protection contre les menaces**. Informations sur les événements consignés pendant l'exécution des modules suivants de l'application :
  - Protection contre les fichiers malicieux
  - Analyse des disques amovibles.
  - Protection contre le chiffrement
  - Protection contre les menaces Internet
  - Protection contre les menaces par emails
  - Protection contre les menaces réseau

- Protection BadUSB
- Gestion du pare-feu
- Contrôle des applications
- Contrôle des appareils
- Détection comportementale
- Protection contre les Exploits
- Contrôle de l'intégrité du système
- Contrôle Internet

- **Tâches à la demande**. Ce rapport contient des informations sur les événements enregistrés lors des tâches d'analyse, des tâches de mise à jour et des tâches de vérification de l'intégrité du système.
- **Prévention de l'exécution** Ce rapport contient des informations sur les événements enregistrés lors de la prévention de l'exécution des objets par les modules EDR Expert (on-premises) et EDR Optimum.

Comment consulter un rapport dans l'interface de l'application

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Rapports**.

   La fenêtre **Rapports** s'ouvre.
3. Sélectionnez le type de rapport requis dans la partie gauche de la fenêtre **Rapports**.

   Le rapport s'affiche dans la partie droite de la fenêtre. Les données des rapports sont présentées dans un tableau qui contient une liste d'événements. Chaque ligne du tableau contient des informations sur un événement distinct. Les attributs d'événement s'affichent dans les colonnes du tableau. Les événements enregistrés lors du fonctionnement de différents modules et tâches ont un ensemble d'attributs différent.

   Par défaut, les événements sont triés par ordre croissant selon les valeurs de la colonne **Date et heure**. Pour faciliter l'utilisation des rapports, vous pouvez modifier la représentation des données à l'écran d'une des manières suivantes :

   - Filtrez la liste des événements par période d'occurrence.
   - utiliser la fonction de recherche d'un événement en particulier ;
4. Si vous souhaitez consulter des informations détaillées sur un événement, sélectionnez l'événement souhaité dans le rapport.

   Une section qui contient les attributs de cet événement s'affiche au bas de la fenêtre.

Collecte de métriques d'état du système

L'application Kaspersky Endpoint Security affecte le système d'exploitation lors de son fonctionnement. Pour analyser ce qui se passe, il est possible de collecter des métriques liées aux performances des applications.

Vous pouvez analyser les métriques dans des outils de visualisation de données tels que Grafana. Les métriques exportées peuvent être publiées vers les principaux systèmes de surveillance, tels que Prometheus et Zabbix.

Configurer la collecte des métriques relatives aux ressources du système d'exploitation utilisées par l'application

```
kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

Où :

`--period` active l'affichage périodique des résultats sur la ligne de commande (avec l'intervalle d'affichage spécifié en secondes).

`--interactive` : affichage interactif (en appuyant sur la touche **Enter**).

L'exécution de cette commande affichera une liste de métriques dans la console.

Liste des métriques

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_system_descriptor_opened_count Jauge	Le nombre de descripteurs actuellement ouverts par le processus kesl. Si le nombre de descripteurs augmente de plus de 250 par heure, nous vous recommandons de contacter le Support technique.
lfs_system_uptime_milliseconds Counter	Le nombre de millisecondes qui se sont écoulées depuis le démarrage du système d'exploitation jusqu'à présent.
lfs_system_memory_usage_bytes étiquette type=virtual Jauge	La quantité de mémoire virtuelle actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_memory_usage_bytes étiquette type=resident Jauge	La quantité de mémoire résidente actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_memory_usage_bytes étiquette type=swap Jauge	Quantité d'espace de swap actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_memory_wd_limits_bytes étiquette type=virtual Jauge	Limite d'utilisation de la mémoire virtuelle du processus kesl.
lfs_system_memory_wd_limits_bytes étiquette type=resident Jauge	Limite d'utilisation de la mémoire résidente du processus kesl.
lfs_system_memory_wd_limits_bytes étiquette type=swap Jauge	Limite d'utilisation de l'espace de swap par le processus kesl.
lfs_system_cpu_usage_milliseconds étiquette type=user Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace utilisateur, depuis le démarrage du processus kesl jusqu'à maintenant. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_system_cpu_usage_milliseconds étiquette type=kernel Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace noyau, depuis le démarrage du processus kesl jusqu'à maintenant. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_cpu_usage_milliseconds étiquette type=total Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace utilisateur et l'espace noyau, depuis le début du processus kesl jusqu'à maintenant. Si le temps CPU du processus kesl dépasse toute autre charge, il est recommandé de contacter le Support technique.
lfs_tcpSynInterceptor_connection_hanging_count Counter	Nombre total de connexions réseau gelées au stade d'établissement de la connexion réseau TCP entre le serveur et le client depuis le début du processus kesl jusqu'à maintenant (les connexions gelées sont celles qui ont attendu que le serveur à distance décide d'autoriser ou non la connexion de 1 seconde à 2 minutes, selon le paramètre système /proc/sys/net/ipv4/tcp_syn_retries). L'augmentation peut être due au fait que le serveur à distance n'est pas disponible ou est absent. Si l'augmentation du nombre de connexions réseau gelées est supérieure à 10 par minute, il est recommandé de contacter le Support technique.
lfs_tcpSynInterceptor_connection_count Jauge	Le nombre de connexions réseau actuellement en attente de connexion au serveur distant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=allow Counter	Nombre total de connexions interceptées qui ont été établies avec succès, depuis le début du processus kesl jusqu'à maintenant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=drop Counter	Le nombre total de connexions interceptées qui n'ont pas réussi à établir une connexion, depuis le début du processus kesl jusqu'à maintenant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=unknown Counter	Nombre total de connexions réseau depuis le début du processus kesl jusqu'à présent avec une décision non traitée du serveur à distance pour autoriser la connexion.
lfs_tcpSynInterceptor_verdict_latency_milliseconds Histogram	Histogramme du temps nécessaire à un serveur à distance pour prendre une décision concernant l'autorisation d'une connexion à partir du moment où un paquet SYN est intercepté jusqu'à ce qu'une décision soit prise à son sujet.
lfs_tproxy_connection_count étiquette direction=inbound Jauge	Le nombre actuel de connexions réseau entrantes interceptées à ce moment.
lfs_tproxy_connection_count étiquette direction=outbound Jauge	Le nombre actuel de connexions réseau sortantes interceptées à ce moment.
lfs_tproxy_connection_processed_count étiquette direction=inbound Counter	Nombre total de connexions réseau entrantes interceptées.
lfs_tproxy_connection_processed_count étiquette direction=outbound Counter	Nombre total de connexions réseau sortantes interceptées.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_tproxy_connection_orphaned_count Counter	Nombre total de connexions (depuis le démarrage des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet) interceptées par l'application Kaspersky Endpoint Security, bien que leur interception n'ait pas été planifiée (par exemple, en raison d'une configuration iptables incompatible ou parce que l'application n'a pas eu le temps de traiter la nouvelle configuration d'interception). De telles connexions seront rejetées. Si le nombre total de ces connexions dépasse 10, cela peut indiquer un dysfonctionnement de l'application ou du système. Il est recommandé de contacter le Support technique.
lfs_tproxy_threadPool_task_count Counter	Nombre total de tâches (nouvelle connexion, nouvelle partie de données, données envoyées, etc.) qui sont entrées dans le pool de threads depuis que les modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet ont commencé à fonctionner. Si la différence entre le nombre total de tâches et le nombre de tâches terminées augmente régulièrement, vous devez ajouter des ressources, configurer des exclusions ou contacter le Support technique.
lfs_tproxy_threadPool_thread_count Jauge	Nombre de threads traitant le mécanisme MITM de l'intercepteur réseau. Les threads sont créés par le gestionnaire de threads pour traiter les connexions. Tous les threads exécutent le même code, dans lequel ils attendent des événements réseau, tels que de nouvelles connexions et des paquets entrants sur les connexions établies.
lfs_tproxy_threadPool_thread_waiting Jauge	Nombre de threads libres sur lfs_tproxy_threadPool_thread_count. Threads en attente sur poll dans le mécanisme MITM de l'intercepteur réseau.
lfs_tproxy_threadPool_task_duration_milliseconds Histogram	Histogramme du temps d'exécution des tâches traitant les connexions interceptées. Si 95 % des tâches prennent plus d'une seconde à s'exécuter, vous devrez peut-être ajouter des ressources, configurer des exclusions ou contacter le Support technique.
lfs_tproxy_socket_count Jauge	Nombre actuel de sockets (sockets d'écoute et sockets de connexion). La connexion interceptée possède 2 sockets de connexion.
lfs_trafficScanning_object_hanging_count Jauge	Le nombre actuel de vérifications d'objets gelées dans le trafic intercepté (les vérifications gelées sont celles qui durent plus d'une minute). Si le nombre total de vérifications d'objets gelées est supérieur à 35, il y a un problème avec les bases de données de l'application. Dans de tels cas, nous vous recommandons de contacter le Support technique.
lfs_trafficScanning_object_duration_milliseconds Histogram	Histogramme du temps de vérification des objets dans le trafic intercepté. Si le temps de vérification de 95 % des objets dépasse 1 seconde, vous devez ajouter des ressources, mettre à jour les bases de données de l'application ou contacter le Support technique. Si le taux de croissance des contrôles de paquets dans le trafic intercepté est de 0 et que la valeur de la métrique lfs_tproxy_threadPool_task_count n'est pas égale à 0, vous devez mettre à jour les bases de données de l'application ou contacter le Support technique.
lfs_fileMonitor_cache_size Jauge	La taille actuelle du cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers. Si la taille actuelle du cache de File Monitor est supérieure à 50 000, nous vous recommandons de contacter le Support technique.
lfs_fileMonitor_cache_hit_count Counter	Le nombre de hits dans le cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers.
lfs_fileMonitor_cache_miss_count Counter	Le nombre d'échecs de cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers.
lfs_faCache_file_count Jauge	Taille actuelle du cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés. Si la taille actuelle du cache des fichiers est supérieure à 100 000, il est recommandé de contacter le Support technique.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_faCache_file_hit_count Counter	Le nombre de hits dans le cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés.
lfs_faCache_file_miss_count Counter	Le nombre d'échecs de cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés.
lfs_faCache_volume_count Jauge	Taille actuelle du cache du point de montage de l'intercepteur fanotify.
lfs_oas_cache_file_count Jauge	La taille actuelle du cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés. Si la taille actuelle du cache des fichiers est supérieure à 100 000, il est recommandé de contacter le Support technique.
lfs_oas_cache_file_hit_count Counter	Le nombre de hits dans le cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés.
lfs_oas_cache_file_miss_count Counter	Le nombre d'échecs du cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés.
lfs_oas_cache_volume_count Jauge	La taille actuelle du cache du point de montage de la Protection contre les fichiers malicieux.
lfs_processManager_cache_size Jauge	Le nombre actuel des processus actifs dans le système qui sont dans le cache.
lfs_processManager_sache_hit_count Counter	Le nombre de hits du cache des processus dans le système.
lfs_processManager_cache_miss_count Counter	Le nombre d'échecs du cache des processus dans le système.
lfs_blockingProcessInterceptor_cache_size Jauge	La taille actuelle du cache des interpréteurs qui peuvent être utilisés pour exécuter des processus. La quantité dépend de l'intensité d'exécution des interprètes sur un appareil particulier. Si la taille actuelle du cache des fichiers est supérieure à 10000, il est recommandé de contacter le Support technique.
lfs_blockingProcessInterceptor_cache_hit_count Counter	Le nombre de hits dans le cache de l'interpréteur.
lfs_blockingProcessInterceptor_cache_miss_count Counter	Le nombre d'échecs du cache des interprètes.
lfs_doc_prevention_cache_file_count Jauge	Taille actuelle du cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'ouverture de documents).
lfs_script_prevention_cache_file_count Jauge	Taille actuelle du cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'exécution de scripts).
lfs_doc_prevention_cache_file_hit_count Counter	Nombre d'accès dans le cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'ouverture de documents).
lfs_script_prevention_cache_file_hit_count Counter	Nombre d'accès dans le cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'exécution de scripts).
lfs_doc_prevention_cache_file_miss_count Counter	Nombre d'échecs dans le cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'ouverture de documents).
lfs_script_prevention_cache_file_miss_count Counter	Nombre d'échecs dans le cache des fichiers de la tâche *Prévention de l'exécution pour les objets* pour les objets qui n'ont pas besoin d'être analysés (lors de l'exécution de scripts).
lfs_doc_prevention_cache_volume_count Jauge	Taille actuelle du cache des points de montage de la tâche "Prévention de l'exécution pour les objets" pour les documents.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_script_prevention_cache_volume_count Jauge	Taille actuelle du cache des points de montage de la tâche "Prévention de l'exécution pour les objets" pour les scripts.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Jauge	Le temps nécessaire à la mise à jour actuelle des métriques pour être effectuée par tous les clients enregistrés dans le registre (en millisecondes).
eka_telemetry_metrics_registry_registered_callbacks Jauge	Le nombre actuel d'appels de fonction de mise à jour de métrique que MetricsRegistry a effectués pour tous les clients enregistrés.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Jauge	Le temps nécessaire pour collecter les valeurs de toutes les métriques du registre (en millisecondes). Si 99 % des valeurs de cette métrique sont supérieures à 1 seconde pendant 10 minutes, nous vous recommandons de contacter le Support technique.

Surveillance de la stabilité des applications

La surveillance de la stabilité des applications de Kaspersky Endpoint Security suit le nombre d'arrêts anormaux des applications et notifie l'administrateur des performances instables des applications.

Comment configurer la surveillance de la stabilité des applications dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security for Linux.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Accédez à l'onglet **Paramètres de l'application**.
4. Choisissez **Paramètres généraux** → **Performances**.
5. Cochez ou décochez la case **Activer la surveillance de la stabilité des applications**. La case est décochée par défaut.

Comment configurer la surveillance de la stabilité des applications dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.
4. Accédez à la section **Paramètres généraux** → **Paramètres de l'application**.
5. Cochez ou décochez la case **Activer la surveillance de la stabilité des applications**. La case est décochée par défaut.

Pour appliquer ce paramètre, vous devez redémarrer l'application et l'Agent d'administration

Si l'application est instable, le message suivant s'affiche dans les propriétés de l'appareil avec l'application installée : *<Number> arrêts anormaux de l'application depuis<date and time>*.

Comment configurer la surveillance de la stabilité des applications en ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de surveillance de la stabilité de l'application Kaspersky Endpoint Security à l'aide des paramètres `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` et `WarnRemovingThreshold` dans le fichier de configuration kesl.ini.

Le paramètre `TrackProductCrashes` vous permet d'activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center lorsque l'application est instable. Le paramètre peut prendre les valeurs suivantes :

- `Yes/true` : activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.
- `No/false` : désactiver l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.

Le paramètre `ProductHealthLogFile` vous permet de spécifier le chemin d'accès au fichier utilisé pour surveiller la stabilité de l'application. Valeur par défaut : /var/opt/kaspersky/kesl/private/kesl_health.log.

Le paramètre `WarnThreshold` permet de préciser l'intervalle de temps (en secondes) pendant lequel l'application doit compter le nombre d'arrêts anormaux avant d'afficher un avertissement d'instabilité. Valeur par défaut : 3600 secondes.

Le paramètre `WarnRemovingThreshold` permet de définir l'intervalle de temps (en secondes) après lequel l'état instable de l'application sera supprimé. Valeur par défaut : 86400 secondes.

Le paramètre `WarnAfter_#_crash` permet de définir le nombre d'arrêts anormaux de l'application, une fois atteint, une notification concernant le fonctionnement instable de l'application s'affiche. Le paramètre peut prendre des valeurs de 0 à 10. Valeur par défaut : 10. Si la valeur est 0, la notification d'instabilité de l'application ne s'affiche pas.

Après avoir apporté des modifications à ce fichier, redémarrez Kaspersky Endpoint Security.

Vérification de l'intégrité des modules d'application

L'application Kaspersky Endpoint Security contient une multitude de modules binaires variés sous forme de bibliothèques de liens dynamiques, de fichiers exécutables, de fichiers de configuration et de fichiers d'interface. Un pirate informatique peut remplacer un ou plusieurs modules ou fichiers exécutables de l'application par d'autres fichiers contenant du code malveillant. Pour empêcher ce remplacement des modules et des fichiers, Kaspersky Endpoint Security peut vérifier l'intégrité des modules de l'application. L'application recherche la présence de modifications non autorisées ou de dommages dans les modules et les fichiers. Si la somme de contrôle du module ou du fichier de l'application est incorrecte, celui-ci est considéré comme endommagé.

Un contrôle d'intégrité est effectué sur les modules d'application suivants, s'ils sont installés sur l'appareil :

- paquet de l'application ;
- paquet de l'interface utilisateur graphique ;
- paquet de l'Agent d'administration de Kaspersky Security Center

- le plug-in Internet d'administration de Kaspersky Endpoint Security
- le plug-in MMC d'administration de Kaspersky Endpoint Security

C'est à l'utilitaire de vérification de l'intégrité qu'il convient de vérifier l'intégrité des modules de l'application. L'utilitaire vérifie l'intégrité des fichiers repris dans des listes spéciales appelées *fichiers de manifeste*. Chaque module de l'application possède son propre fichier de manifeste. Celui reprend la liste des fichiers de l'application dont l'intégrité est importante au fonctionnement correct de ce module. Les fichiers de manifeste possèdent une signature numérique. Leur intégrité est vérifiée également.

Pour exécuter l'utilitaire de vérification de l'intégrité sur les appareils exécutant les systèmes d'exploitation Linux, un compte avec les droits root est requis.

L'utilitaire de vérification de l'intégrité est installé avec l'application et se trouve à l'emplacement suivant :

- Dans le cadre du paquet de l'application (integrity_checker) : /opt/kaspersky/kesl/bin/integrity_checker.
- Le plug-in MMC d'administration de Kaspersky Endpoint Security (integrity_checker.exe) comprend :
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<numéro de version>.plg\integrity_checker.exe : pour les systèmes d'exploitation 32 bits ;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<numéro de version>.plg\integrity_checker.exe : pour les systèmes d'exploitation 64 bits.

Les fichiers de manifeste se trouvent dans les emplacements suivants :

- Pour vérifier l'intégrité du paquet de l'application : /opt/kaspersky/kesl/bin/integrity_check.xml.
- Pour vérifier l'intégrité du paquet de l'interface utilisateur graphique : /opt/kaspersky/kesl/bin/gui_integrity_check.xml.
- Pour vérifier l'Agent d'administration :
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml : pour les systèmes d'exploitation 32 bits ;
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml : pour les systèmes d'exploitation 64 bits ;
- Pour vérifier le plug-in MMC d'administration de Kaspersky Endpoint Security
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_check.xml : pour les systèmes d'exploitation 32 bits ;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_check.xml : pour les systèmes d'exploitation 64 bits.

Pour vérifier l'intégrité du module de la solution, vous devez exécuter l'utilitaire à partir du dossier d'emplacement de l'utilitaire pour ce module.

Vérifier l'intégrité du paquet de l'application

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type
kds-with-filename
```

Vérifier l'intégrité du paquet de l'interface graphique

```
integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-
with-filename
```

Vérifier l'intégrité du plug-in MMC d'administration de Kaspersky Endpoint Security

```
integrity_checker.exe [<path to manifest file>]
```

Vérifier l'intégrité de l'Agent d'administration

```
integrity_checker <path to manifest file>
```

Par défaut, le chemin d'accès utilisé est celui du fichier de manifeste situé dans le répertoire où se trouve l'utilitaire de vérification de l'intégrité.

Vous pouvez démarrer l'utilitaire avec les paramètres facultatifs suivants :

- `--crl <directory>` correspond au chemin d'accès au répertoire contenant la liste de révocation des certificats.
- `--verbose` : affichage détaillé des actions effectuées et des résultats. Si vous ne spécifiez pas ce paramètre, seules les erreurs, les objets qui n'ont pas réussi la vérification et les statistiques de l'analyse récapitulative seront fournis.
- `--trace <file name>` consigne les événements survenus pendant l'analyse dans le fichier spécifié avec le niveau de journalisation DEBUG.
- `--signature-type kds` correspond au type de signature à vérifier (cette option est requise pour vérifier le plug-in Internet d'administration de Kaspersky Endpoint Security).
- `--signature-type kds-with-filename` correspond au type de signature à vérifier (ce paramètre est requis pour vérifier le paquet de l'application et le paquet de l'interface graphique).
- `--single_file <file name>` vérifie uniquement le fichier spécifié dans le manifeste et ignore tous les autres objets du manifeste.
- `--version` : afficher la version de l'utilitaire sans effectuer de vérification de l'intégrité.

Afficher toutes les options disponibles de l'outil de vérification de l'intégrité

```
integrity_checker --help
```

Le résultat de la vérification du fichier de manifeste s'affiche de la manière suivante :

- `SUCCEEDED` : l'intégrité des fichiers est confirmée (code retour 0).
- `FAILED` : l'intégrité des fichiers n'est pas confirmée (le code retour n'est pas 0).

En cas de violation de l'intégrité de l'application ou de l'Agent d'administration lors du lancement de l'application, l'application Kaspersky Endpoint Security génère l'événement à ce sujet dans le journal des événements et dans Kaspersky Security Center.

Contrôle de l'accès à l'application

Le contrôle d'accès dans Kaspersky Endpoint Security repose sur une stratégie de Role Based Access Control (RBAC). Pour accorder à un utilisateur certains droits ou l'accès à une ressource, vous devez lui attribuer les rôles correspondants. Un *rôle* est un ensemble de droits et privilèges pour l'administration de l'application.

Les rôles utilisateur facilitent et accélèrent la gestion courante des droits d'accès. Les droits d'accès d'un rôle sont configurés conformément aux tâches standard et aux descriptions de poste des utilisateurs.

L'application a besoin de privilèges élevés dans le système d'exploitation pour protéger les appareils. L'application requiert les privilèges root pour exécuter certaines de ses fonctions de sécurité de base.

Le modèle d'accès basé sur les rôles de l'application inclut le rôle Administrateur (admin). Dans certains cas, les actions des utilisateurs ayant le rôle Administrateur peuvent entraîner l'exécution d'opérations avec les privilèges du superutilisateur du système d'exploitation (root).

Le rôle Administrateur doit uniquement être accordé à des utilisateurs de confiance. La compromission ou l'utilisation abusive de ce rôle Administrateur entraîne la compromission de l'appareil dans son ensemble et peut avoir un impact sur la sécurité, l'intégrité ou les performances de l'infrastructure de votre organisation, ainsi que sur les données utilisateur.

L'attribution du rôle Administrateur relève de la responsabilité du propriétaire du système et doit être effectuée conformément à la stratégie de contrôle d'accès de votre organisation et au niveau de confiance accordé aux utilisateurs concernés.

Rôles prédéfinis

L'accès aux fonctions de l'application Kaspersky Endpoint Security via la ligne de commande est octroyé à l'utilisateur conformément à son rôle. Un *rôle* est un ensemble de droits et privilèges pour l'administration de l'application.

Quatre groupes d'utilisateurs système sont créés dans le système d'exploitation :

- kesladmin
- kesluser
- keslaudit
- nokesl

Lorsque vous attribuez un rôle de l'application à un utilisateur système, l'utilisateur est ajouté au groupe correspondant (voir le tableau ci-dessous). Lorsque vous retirez un rôle à un utilisateur, cet utilisateur est retiré du groupe correspondant.

Après l'attribution ou la révocation d'un rôle, vous devez redémarrer l'application (le processus kesl) et son interface graphique (le processus kesl-gui).

Rôles et groupes d'utilisateurs

Nom du rôle	Rôle dans l'application	Groupe d'utilisateurs du système d'exploitation	Autorisations
Administrateur	admin	kesladmin	Gérez les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`. Gérer les licences d'application. Attribuer n'importe quel rôle à n'importe quel utilisateur. Révocation de rôles d'utilisateurs (un administrateur ne peut pas se retirer le rôle admin). Afficher et gérer les stockages des utilisateurs.
Utilisateur	user	kesluser	Gérer uniquement les tâches d'analyse personnalisée des fichiers. Démarrer et arrêter les tâches de mise à jour. Envoi de fichiers vers la Sandbox pour analyse Afficher les rapports des tâches personnalisées. Afficher des événements spécifiques communs à tous les utilisateurs de l'application.
Auditeur	audit	keslaudit	Affichage des paramètres de l'application. Afficher l'état de l'application. Afficher toutes les tâches, leurs paramètres et leurs planifications. Afficher tous les événements. Afficher tous les objets dans la sauvegarde.
–	–	nokesl	Le rôle dans l'application n'est pas attribué, il n'y a pas de droits.

Comment attribuer ou révoquer un rôle utilisateur

Les rôles définissent les droits d'un utilisateur et les actions que celui-ci peut exécuter dans le système. Seuls les utilisateurs dotés du rôle Administrateur (kesladmin) peuvent gérer les rôles. Il est recommandé de créer au moins un utilisateur doté du rôle Administrateur sur l'appareil protégé afin d'éviter que l'application soit administrée par des utilisateurs disposant de privilèges root.

Affichage d'une liste d'utilisateurs et de rôles

```
kesl-control --get-user-list
```

Attribuer un rôle à un utilisateur

```
kesl-control --grant-role <admin|user|audit> <user name>
```

Exemple d'attribution du rôle audit à l'utilisateur test15

```
kesl-control --grant-role audit test15
```

Révoquer un rôle d'un utilisateur

```
kesl-control --revoke-role <role> <user name>
```

Exemple de révocation du rôle audit de l'utilisateur test15

```
kesl-control --revoke-role audit test15
```

Zones fonctionnelles RBAC dans Kaspersky Security Center

Par défaut, les utilisateurs dotés du rôle « Administrateur de Kaspersky Endpoint Security » dans le système d'administration de Kaspersky Security Center ont accès à toutes les fonctionnalités de Kaspersky Endpoint Security.

Vous pouvez sélectionner l'un des niveaux d'accès prédéfinis suivants aux fonctionnalités de Kaspersky Endpoint Security pour un utilisateur ou un groupe de Kaspersky Endpoint Security :

- **Lecture** permet de consulter les paramètres généraux de Kaspersky Endpoint Security et les paramètres des modules de Kaspersky Endpoint Security.
- **Modification** permet de consulter et de modifier les paramètres généraux de Kaspersky Endpoint Security et les paramètres des modules de Kaspersky Endpoint Security.
- **Exécution** permet de démarrer et d'arrêter les tâches de Kaspersky Endpoint Security.
- **Exécution d'opérations sur les sélections d'appareils** permet de démarrer et d'arrêter les tâches de Kaspersky Endpoint Security pour une sélection d'appareils.

Vous pouvez également configurer des autorisations d'accès avancées : autoriser ou refuser l'accès aux fonctions de Kaspersky Endpoint Security.

Comment configurer les autorisations d'accès aux fonctions de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Utilisateurs et rôles** → **Rôle**.
2. Sélectionnez le rôle pour lequel vous souhaitez configurer les zones fonctionnelles.

   Si nécessaire, vous pouvez ajouter un nouveau rôle. Consultez l'aide de Kaspersky Security Center pour plus de détails.
3. Configurez les droits d'accès à l'application Kaspersky Endpoint Security.
4. Cliquez sur le bouton **Enregistrer**.

Autorisations d'accès aux fonctions de Kaspersky Endpoint Security

Zone fonctionnelle	Fonctionnalités de Kaspersky Endpoint Security
Fonctionnalité de base	Mise à jour des bases et des modules de l'application Annulation de la mise à jour des bases Inventaire Protection BadUSB Contrôle de l'intégrité du système Vérification de l'intégrité du système Paramètres de détection Kaspersky Security Network Interaction avec l'utilisateur Performances Paramètres du réseau Analyser les conteneurs. Support technique Rapports et stockage Intégration avec KSC Source de télémétrie et mode auditd (paramètres d'interaction avec le système d'exploitation) Paramètres des événements Mode Light Agent Ajout d'une clé
Contrôle des applications	Contrôle des applications
Contrôle des appareils	Contrôle des appareils
Chiffrement des données	Accorder un accès temporaire à un appareil (Contrôle des appareils)
Exclusions de l'analyse pour l'application	Zone de confiance : • Spécifie les adresses Internet de confiance • Adresses IP de confiance • Fenêtre Ports contrôlés • Certificats racines de confiance • Domaines de confiance • Points de montage de confiance • Exclusions de l'interception du trafic • Applications de confiance • Exclusions de l'analyse des logiciels malveillants • Appareils de confiance

Zone fonctionnelle	Fonctionnalités de Kaspersky Endpoint Security
Detection and Response	Agents intégrés : • Managed Detection and Response • Endpoint Detection and Response • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Intégration avec KUMA. Actions de réponse : • Terminer le processus • Démarrage du processus • analyse IOC ; • Réception d'un fichier depuis l'appareil • Placer le fichier en quarantaine • Suppression d'un fichier de votre appareil • Isolation réseau • Prévention de l'exécution des objets • Paramètres de la télémétrie
Prévention des intrusions	Détection comportementale Protection contre les Exploits Protection contre le chiffrement Protection contre les menaces réseau Gestion du pare-feu
Modules de protection	Analyse des logiciels malveillants Analyse des zones critiques Protection contre les fichiers malicieux Protection contre les menaces par emails Analyse des disques amovibles Protection contre les menaces Internet
Contrôle Internet	Contrôle Internet

Recommandations relatives aux rôles types des appareils protégés

Poste de travail

Si vous installez l'application sur un poste de travail, nous vous recommandons d'installer également l'interface graphique de l'application.

Après l'installation de l'application :

- Activez la Protection contre les menaces Internet.
- Si l'appareil ne dispose pas d'une connexion directe à Internet, sélectionnez la validation locale des certificats dans les paramètres d'analyse du trafic réseau à l'aide de l'une des options suivantes :
  - Dans la Web Console, sous **Analyse des connexions chiffrées**, cliquez sur le bouton **Paramètres**, puis définissez **Stratégie de vérification du certificat** sur **Vérification locale**.
  - Dans la Console d'administration, sous **Paramètres des connexions chiffrées**, définissez **Stratégie de vérification du certificat** sur **Vérification locale**.

- Localement sur l'appareil à l'aide de la ligne de commande :

  ```
  kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
  ```

  L'application n'utilisera pas Internet pour vérifier les certificats.

- Configurez une exclusion de l'interception des opérations sur les fichiers (exclusion globale) pour tous les répertoires distants montés sur l'appareil à l'aide des protocoles Samba et NFS.

Serveur de fichiers

Après l'installation de l'application :

1. Assurez-vous que l'analyse des archives est désactivée dans les paramètres de la Protection contre les fichiers malicieux. Cette option est sélectionnée par défaut.
2. Créez une tâche *Analyse des logiciels malveillants* avec les paramètres suivants :
   - analyse des archives : activée
   - planification de la tâche : pendant les heures de charge minimale

Serveur Web

Kaspersky Endpoint Security n'est pas conçu pour protéger les serveurs Web. Pour protéger les serveurs Web, nous vous recommandons d'utiliser Kaspersky NGFW et Kaspersky Web Traffic Security.

Si vous utilisez Kaspersky Endpoint Security sur un serveur Web, si le serveur utilise le protocole HTTPS et si la charge client est élevée, la Protection contre les menaces Internet peut augmenter considérablement l'utilisation des ressources système. Cela se produit parce que l'application décrypte et vérifie le trafic HTTPS.

Analysez l'évolution de la charge sur le serveur Web pendant le fonctionnement de la Protection contre les menaces Internet. Vous pouvez configurer des exclusions pour optimiser les paramètres et éliminer les problèmes de compatibilité.

Serveur proxy

Après l'installation de l'application, désactivez les modules Protection contre les menaces Internet et Protection contre les menaces réseau sur l'appareil qui fait office de serveur proxy ou d'équilibreur de charge.

Serveur avec conteneurisation

Après l'installation de l'application, désactivez les modules Protection contre les menaces Internet, Protection contre les menaces réseau et Gestion du pare-feu sur les serveurs utilisés pour les services de conteneurisation. Pour protéger les environnements de conteneurs, vous pouvez utiliser l'application Kaspersky Container Security.

Serveur de base de données

Configurez des exclusions globales pour les répertoires de travail du système de gestion de base de données.

Contactez votre administrateur de SGBD pour obtenir la liste des répertoires de travail dans votre infrastructure.

Les exemples de chemins suivants sont destinés au système d'exploitation Ubuntu. Dans les autres systèmes d'exploitation, les répertoires peuvent différer.

Recommandations pour les SGBD courants

PostgreSQL. Il est essentiel d'éliminer complètement toute latence lors des opérations sur les fichiers de données et les journaux d'écriture anticipée (fichiers WAL). Nous vous recommandons également d'exclure les opérations sur les fichiers des processus PostgreSQL et des espaces de table (voir l'exemple ci-dessous). Dans une installation PostgreSQL standard, ces fichiers se trouvent dans les répertoires suivants :

- Statistiques et requêtes parallèles : `/dev/shm`
- Données : `/var/lib/postgresql/<PostgreSQL version>/main`
- Fichiers WAL : `/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- Fichiers exécutables : `/usr/lib/postgresql/<PostgreSQL version>/bin/`.

Postgres Pro. Suivez les recommandations relatives à PostgreSQL. De plus, ajoutez le répertoire `/var/lib/pgpro/<Postgres Pro version>/data` aux exclusions.

Oracle Database. Vous pouvez obtenir la liste des répertoires de travail de toutes les bases de données à partir du fichier de configuration `/etc/oratab`.

ScyllaDB. Lorsque vous utilisez les modules Protection contre les menaces Internet et Protection contre les menaces réseau, utilisez le mode eBPF d'interception du trafic. Pour gérer le mode de mise en cache des solutions Detection and Response, utilisez la valeur par défaut du paramètre `UseIncreasedXdrEventsCache=yes` dans le fichier de configuration kesl.ini.

Exemple de configuration des exclusions globales pour les répertoires de travail PostgreSQL

Si vous utilisez un mécanisme basé sur la *technologie fanotify* pour intercepter les événements système, les répertoires de fichiers du SGBD doivent être des points de montage. Si vous utilisez le *module de noyau mis à jour* pour intercepter les événements système, vous n'avez pas besoin de créer de points de montage.

Pour créer des points de montage :

1. Vérifiez si les répertoires contenant le fichier de base de données sont des points de montage :

```
mount
```

Si les répertoires ne figurent pas dans la sortie de la commande mount :

a. Créez un point de montage :

```
mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
```

Vous n'avez pas besoin de créer un point de montage distinct pour le répertoire contenant les fichiers WAL, car il est imbriqué dans le répertoire de données.

b. Ajoutez la ligne suivante au fichier /etc/fstab afin que le point de montage nouvellement créé soit conservé dans le système après le redémarrage :

```
/var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
defaults,bind 0 0
```

2. Redémarrez le service PostgreSQL :

```
systemctl restart postgresql
```

Pour configurer des exclusions globales pour les répertoires de travail :

1. Ajoutez les répertoires aux exclusions globales :

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
version>/main/pg_wal
kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
```

2. Si vous utilisez des tablespaces, ajoutez-les également aux exclusions :

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
```

3. Redémarrez l'application pour appliquer les exclusions globales :

```
systemctl restart kesl
```

Mise à jour des bases et des modules de l'application

La mise à jour des bases de données et des modules de Kaspersky Endpoint Security garantit l'actualité de la protection de votre appareil. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de données de l'application Kaspersky Endpoint Security contiennent des informations relatives aux menaces et aux moyens de les neutraliser. Afin de pouvoir détecter les menaces rapidement, vous êtes vivement encouragé à mettre à jour régulièrement les bases de données et les modules de l'application.

Pour pouvoir bénéficier de ces mises à jour des bases de données régulières, votre licence doit être active. Sans licence en cours, vous ne pourrez réaliser qu'une seule mise à jour.

Si le déploiement de l'application a réussi et que vous avez choisi de mettre à jour les bases de données à l'étape de configuration initiale, les bases de données sont à jour après l'installation de l'application. Vous pouvez obtenir des informations sur l'état des bases de données lors de la consultation de l'état de la protection de l'appareil dans Kaspersky Security Center en vérifiant les états des appareils clients, ainsi que sur la ligne de commande à l'aide de la commande `kesl-control --app-info`. Si les bases de données ne sont pas à jour, vous devez configurer et lancer une mise à jour des bases de données.

Configuration des mises à jour des bases de données et des modules

1. **Sélection du schéma de distribution des mises à jour et de la source de mise à jour**

   Une *source des mises à jour* est une ressource qui contient les mises à jour des bases de données et des modules de l'application Kaspersky Endpoint Security. La source de mise à jour peut être l'un des éléments suivants : les serveurs de mise à jour de Kaspersky ; le stockage du Serveur d'administration de Kaspersky Security Center ; un serveur FTP, HTTP ou HTTPS ; un répertoire local ou réseau monté par l'utilisateur à l'aide des protocoles Samba ou NFS.

   Si Kaspersky Endpoint Security est utilisé en mode Light Agent, les bases de données des machines virtuelles protégées sont mises à jour à partir du répertoire de la SVM.

2. **Configuration de la tâche de mise à jour des bases de données**

   La tâche *Update* télécharge le paquet de mise à jour et installe les mises à jour des bases de données et des modules de l'application sur l'appareil.

La fonctionnalité des mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) peut ne pas être disponible dans le logiciel aux États-Unis.

Lors de la réalisation d'une mise à jour, les objets suivants sont téléchargés et installés sur l'appareil :

- Les bases de Kaspersky Endpoint Security. Les bases de données de l'application comprennent les règles de détection des applications malveillantes, la description des attaques de réseau, les bases de données d'adresses Internet malveillantes et de phishing, les bases de données de bannières, les bases de données de spam ainsi que d'autres données.
- Modules de l'application. Les mises à jour des modules servent à éliminer les vulnérabilités de l'application et à améliorer les méthodes de protection de l'appareil. Les mises à jour des modules peuvent modifier le comportement des modules de l'application et ajouter de nouvelles fonctions.

Vous pouvez également recevoir des mises à jour d'applications installées automatiquement (correctifs automatiques). Les correctifs automatiques contiennent des corrections et des améliorations pour l'application.

Pendant la mise à jour, les modules de l'application et les bases de données installés sur votre ordinateur sont comparés à leurs versions à jour disponibles dans la source de mise à jour. Si vos bases de données et les modules de l'application diffèrent des versions respectives à jour, la portion manquante des mises à jour est installée sur l'appareil.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo). L'espace disque nécessaire peut atteindre 3 Go.

Articles utiles

Résolution des problèmes liés aux mises à jour des bases de données et des modules de l'application

Que faire si vous obtenez l'état : "Une mise à jour de l'application ou du module cryptossl a été installée. Redémarrez l'application."

Comment sélectionner la source de mise à jour et le schéma de distribution

Sélection d'une source de mise à jour de Kaspersky Endpoint Security

Une *source des mises à jour* est une ressource qui contient les mises à jour des bases de données et des modules de l'application Kaspersky Endpoint Security.

La source de mise à jour peut être l'un des éléments suivants : les serveurs de mise à jour de Kaspersky, le stockage du Serveur d'administration de Kaspersky Security Center, un répertoire local ou réseau (SMB/NFS) monté par l'utilisateur, des serveurs FTP, HTTP ou HTTPS. Lorsque vous choisissez votre propre serveur HTTPS comme source de mise à jour, vous devez vous assurer qu'il dispose de la chaîne de certificats correcte. Un certificat auto-signé peut uniquement être utilisé comme certificat racine dans une chaîne de certificats. Dans ce cas, vous devez l'ajouter à la liste des certificats de confiance sur l'appareil.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, les bases de données des machines virtuelles protégées sont mises à jour à partir du répertoire de la SVM.

Si plusieurs ressources sont sélectionnées comme sources de mise à jour, Kaspersky Endpoint Security tente de s'y connecter l'une après l'autre, en commençant par le début de la liste, et exécute la tâche de mise à jour en récupérant le paquet de mise à jour depuis la première source disponible. Vous pouvez configurer le délai d'attente de réponse d'une source de mise à jour sélectionnée lors de la tentative de connexion à celle-ci. Si aucune réponse n'est reçue de la source de mise à jour dans le délai spécifié, l'application contacte une autre source de mise à jour spécifiée.

Sélection d'un schéma de distribution des mises à jour

Kaspersky Endpoint Security prend en charge les schémas de distribution suivants pour les mises à jour des bases et des modules d'application :

Mise à jour centralisée.

Si vous utilisez Kaspersky Security Center pour administrer de manière centralisée la protection des appareils dans votre organisation, nous vous recommandons de configurer les mises à jour centralisées des bases de données. La mise à jour centralisée permet de réduire le trafic Internet externe et garantit la commodité du contrôle des mises à jour.

La mise à jour centralisée se déroule selon les étapes suivantes :

1. Chargement du paquet de mise à jour dans le stockage au sein du réseau de l'organisation.

   Vous pouvez utiliser le stockage du Serveur d'administration de Kaspersky Security Center comme stockage. Le paquet de mise à jour est téléchargé dans le stockage du Serveur d'administration via la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* du Serveur d'administration.

2. Distribuer le paquet de mise à jour aux appareils clients.

   Le paquet de mise à jour est distribué aux appareils clients via *tâche de mise à jour* de Kaspersky Endpoint Security. Dans les paramètres de la tâche, sélectionnez Kaspersky Security Center comme source de mise à jour.

Mise à jour depuis les serveurs de mises à jour Kaspersky

Les serveurs de mise à jour Kaspersky sont répartis à travers le monde, ce qui garantit la haute fiabilité des mises à jour. Si une mise à jour ne peut être réalisée depuis un serveur, l'application passe au serveur suivant. Les mises à jour sont téléchargées via le protocole HTTPS. Pour plus d'informations sur les serveurs de mise à jour de Kaspersky, consultez la Base de connaissances du Support technique.

Mise à jour depuis un répertoire local ou réseau (SMB/NFS) monté par l'utilisateur, ou depuis un serveur FTP, HTTP ou HTTPS

La source de mise à jour personnalisée doit contenir des paquets de mise à jour préalablement téléchargés (ce que vous pouvez faire, par exemple, à l'aide de Kaspersky Update Utility). Lorsque vous choisissez votre propre serveur HTTPS comme source de mise à jour, vous devez vous assurer qu'il dispose de la chaîne de certificats correcte. Un certificat auto-signé peut uniquement être utilisé comme certificat racine dans une chaîne de certificats. Dans ce cas, vous devez l'ajouter à la liste des certificats de confiance sur l'appareil. Vous pouvez indiquer la sources de mises à jour personnalisée dans les paramètres de la tâche *Mise à jour*. Pour plus d'informations sur la création de sources de mise à jour personnalisées, consultez l'aide de Kaspersky Security Center.

Les mises à jour sont téléchargées depuis les serveurs de mise à jour Kaspersky ou depuis d'autres serveurs FTP, HTTP ou HTTPS via les protocoles réseau standard. Les paramètres de la connexion Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, spécifiez les paramètres du serveur proxy.

Procédure de configuration de la tâche de mise à jour des bases de données

La tâche *Update* télécharge le paquet de mise à jour et installe les mises à jour des bases de données et des modules de l'application sur l'appareil.

Mise à jour des bases de données dans Kaspersky Security Center

Dans Kaspersky Security Center, la tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Update* lors de l'exécution de l'Assistant, vous devez installer le plug-in d'administration de Kaspersky Endpoint Security.

Vous pouvez utiliser une tâche de groupe *Mise à jour* créée automatiquement ou créer et exécuter des tâches personnalisées de mise à jour de groupe et locales à l'aide de Web Console ou de la Console d'administration.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, les bases de données des machines virtuelles protégées sont mises à jour à l'aide d'une tâche locale spéciale *Mise à jour*, dans laquelle le répertoire sur la SVM est indiqué comme source de mise à jour. La tâche de mise à jour démarre automatiquement. Vous ne pouvez pas supprimer cette tâche et modifier ses paramètres. La mise à jour des bases de données et des modules de l'application à l'aide des tâches créées dans Kaspersky Security Center n'est pas prise en charge.

Comment configurer et exécuter une tâche de mise à jour dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Dans la liste des tâches, sélectionnez la tâche de mise à jour de Kaspersky Endpoint Security, puis cliquez sur le nom de la tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Sources de mise à jour**, sélectionnez la source à partir de laquelle l'application recevra les mises à jour des bases de données et des modules, en fonction du scénario de mise à jour utilisé.

   La liste des sources de mises à jour contient deux sources : les serveurs de mise à jour de Kaspersky et Kaspersky Security Center. La colonne **État** indique si l'application utilise cette source de mises à jour lors de l'exécution de la tâche. Vous pouvez ajouter d'autres sources de mises à jour à la liste en cliquant sur le bouton **Ajouter**. Comme sources de mise à jour, vous pouvez indiquer des répertoires sur des serveurs FTP, HTTP et HTTPS ou des répertoires sur tout appareil monté sur l'appareil client protégé, y compris des répertoires sur des appareils distants montés via les protocoles Samba ou NFS. Si une mise à jour ne peut pas être réalisée au départ d'une source de mise à jour, l'application Kaspersky Endpoint Security passe à la suivante. L'application s'adresse aux sources de mises à jour dans l'ordre où celles-ci apparaissent dans le tableau.

5. Dans la fenêtre des propriétés de la tâche, sélectionnez l'onglet **Programmation** et configurez la programmation de l'exécution de la tâche de mise à jour. Par défaut, le lancement en mode manuel est sélectionné pour la tâche.

   Si vous avez sélectionné **Kaspersky Security Center** comme source de mise à jour, dans la liste déroulante **Lancement de la tâche**, sélectionnez **Lors du téléchargement des mises à jour dans le référentiel**. Pour plus d'informations sur la planification des tâches, consultez l'aide de Kaspersky Security Center.

6. Enregistrez vos modifications.

La tâche s'exécutera selon le calendrier configuré. Vous pouvez également exécuter la tâche manuellement.

Comment configurer et exécuter une tâche de mise à jour dans la Console d'administration

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur les appareils faisant partie d'un groupe d'administration spécifique, sélectionnez ce groupe d'administration dans l'arborescence de la console, puis sélectionnez l'onglet **Tâches** dans l'espace de travail.

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur un ou plusieurs appareils (tâches pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console.

2. Dans la liste des tâches, sélectionnez une tâche de mise à jour, puis double-cliquez dessus pour ouvrir la fenêtre des propriétés de la tâche.

3. Dans la fenêtre des propriétés de la tâche, ouvrez la liste de gauche et sélectionnez l'option **Sources des mises à jour**.

4. Dans le tableau, sélectionnez la source de mise à jour à partir de laquelle l'application recevra les mises à jour de la base de données et des modules, en fonction du schéma de mise à jour utilisé.

   La liste des sources de mises à jour contient deux sources : les serveurs de mise à jour de Kaspersky et Kaspersky Security Center. La colonne **État** indique si l'application utilise cette source de mises à jour lors de l'exécution de la tâche. Vous pouvez ajouter d'autres sources de mises à jour à la liste en cliquant sur le bouton **Ajouter**. Vous pouvez désigner des serveurs FTP, HTTP ou HTTPS en tant que sources de mises à jour. Si une mise à jour ne peut pas être réalisée au départ d'une source de mise à jour, l'application Kaspersky Endpoint Security passe à la suivante. L'application s'adresse aux sources de mises à jour dans l'ordre où celles-ci apparaissent dans le tableau.

5. Sélectionnez la section **Paramètres** et configurez d'autres paramètres de mise à jour.

6. Sélectionnez l'onglet **Planification** et configurez la planification d'exécution de la tâche de mise à jour. Par défaut, le lancement en mode manuel est sélectionné pour la tâche.

   Si vous avez sélectionné **Kaspersky Security Center** comme source de mise à jour, dans la liste déroulante **Lancement planifié**, sélectionnez **Lors du téléchargement des mises à jour dans le référentiel**. Pour plus d'informations sur la planification des tâches, consultez l'aide de Kaspersky Security Center.

7. Cliquez sur le bouton **Appliquer** ou sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la tâche>** pour enregistrer vos modifications.

La tâche s'exécutera selon le calendrier configuré. Vous pouvez également exécuter la tâche manuellement.

Mise à jour des bases de données via la ligne de commande

Sur la ligne de commande, vous pouvez mettre à jour les bases et modules d'application à l'aide de la tâche prédéfinie *`Update`* ou créer des tâches définies par l'utilisateur de type `Update`.

Vous pouvez gérer les tâches de mise à jour manuelles (les démarrer, les arrêter, les suspendre et les reprendre), configurer la programmation de la tâche et gérer les paramètres de mise à jour en modifiant les paramètres des tâches.

Comment créer et configurer une tâche de mise à jour via la ligne de commande

Sur la ligne de commande, vous pouvez créer et configurer une tâche personnalisée de mise à jour de deux manières :

- Créer une tâche en spécifiant tous ses paramètres dans un fichier de configuration.
- Créer une tâche avec les paramètres par défaut, puis configurer ses paramètres.

```
Créer une tâche de mise à jour avec les paramètres provenant d'un fichier de configuration

kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

Où :

- `<path to file>` correspond au chemin d'accès complet au fichier de configuration contenant les paramètres que vous souhaitez utiliser pour la tâche.
- `--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

  Exemple de fichier de configuration :

  ```
  ConnectionTimeout=10
  ApplicationUpdateMode=DownloadOnly
  [Sources.item_0000]
  Enabled=Yes
  SourceType=Custom
  URL=https://s00.upd.kaspersky.com
  ```

Pour créer et configurer une tâche de mise à jour avec les paramètres par défaut :

1. Créez une tâche en exécutant la commande suivante :

   ```
   kesl-control --create-task <nom de la tâche de mise à jour> --type Update
   ```

   où `<update task name>` correspond au nom que vous souhaitez attribuer à la nouvelle tâche de mise à jour.

   Cette commande crée une tâche de mise à jour avec les paramètres par défaut.

2. Si nécessaire, gérez les paramètres de la tâche de mise à jour en exécutant la commande suivante :

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. Si nécessaire, gérez les paramètres de programmation de la tâche de mise à jour en exécutant la commande suivante :

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. Vérifiez les valeurs actuelles des paramètres de la tâche en exécutant la commande suivante :

   ```
   kesl-control --get-settings <update task ID|name>
   ```

Mise à jour des bases dans l'interface graphique de l'application

Comment lancer ou arrêter une tâche de mise à jour dans l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour**.

   La fenêtre **Mise à jour** s'ouvre.

3. Exécutez une des actions suivantes :

   - Si vous voulez démarrer une tâche, cliquez sur le bouton **Démarrer** sous la tâche d'analyse que vous voulez démarrer.

     La progression de la tâche de mise à jour en cours s'affiche.

   - Si vous souhaitez arrêter une tâche, cliquez sur le bouton **Arrêter** situé sous la tâche que vous souhaitez arrêter.

     La tâche de mise à jour s'arrête.

4. Si vous souhaitez afficher le rapport d'une tâche, cliquez sur le bouton **Afficher le rapport**.

Procédure de mise à jour à l'aide de Kaspersky Update Utility

Afin d'économiser le trafic Internet, vous pouvez configurer les mises à jour des bases de données et des modules de l'application sur les appareils du réseau local de l'organisation à partir d'un répertoire partagé à l'aide de Kaspersky Update Utility. Pour ce faire, un des appareils du réseau local de l'organisation doit recevoir les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou depuis les serveurs de mise à jour de Kaspersky, puis copier les paquets de mise à jour reçus dans le répertoire partagé à l'aide de l'utilitaire. Les autres appareils du réseau local de l'organisation peuvent alors recevoir le paquet de mise à jour depuis ce répertoire partagé.

Pour configurer Kaspersky Security Center afin qu'il mette à jour les bases de données à partir d'un répertoire partagé à l'aide de l'utilitaire Kaspersky Update Utility :

1. Installez Kaspersky Update Utility sur l'un des appareils du réseau local de l'organisation.

   Vous pouvez télécharger le paquet de distribution de Kaspersky Update Utility depuis le site Internet du Support technique de Kaspersky.

2. Configurez la copie du paquet de mise à jour dans le répertoire partagé dans les paramètres de Kaspersky Update Utility.

   Sélectionnez la source de mises à jour (par exemple, le stockage du Serveur d'administration) et le répertoire partagé dans lequel Kaspersky Update Utility va copier les paquets de mise à jour. Pour des informations détaillées sur l'utilisation de Kaspersky Update Utility, consultez la Base de connaissances Kaspersky.

3. Configurez la mise à jour des bases et des modules de l'application à partir du répertoire partagé indiqué vers les autres appareils du réseau local de l'organisation :

   a. Ouvrez les propriétés de la tâche **Update** qui sera exécutée sur l'appareil requis à l'aide de Web Console ou de la Console d'administration.

   b. Dans les propriétés de la tâche, accédez à la section **Sources de mises à jour**.

   c. Sélectionnez l'option **Autres sources sur le réseau local ou sur Internet** dans le groupe **Source des mises à jour**.

   d. Dans le tableau des sources de mises à jour, cliquez sur le bouton **Ajouter** et précisez le chemin d'accès au répertoire partagé.

      L'adresse de la source des mises à jour doit correspondre à l'adresse renseignée dans les paramètres de Kaspersky Update Utility.

e. Cochez la case **Utiliser cette source**, puis cliquez sur **OK**.

f. Dans le tableau des sources de mises à jour, définissez l'ordre d'utilisation à l'aide des boutons **Haut** et **Bas**.

g. Enregistrez les modifications apportées aux paramètres de la tâche.

Pour configurer dans la ligne de commande les mises à jour des bases de données à partir d'un répertoire partagé à l'aide de Kaspersky Update Utility :

1. Installez Kaspersky Update Utility sur l'un des appareils du réseau local de l'organisation.

   Vous pouvez télécharger le paquet de distribution de Kaspersky Update Utility depuis le site Internet du Support technique de Kaspersky.

2. Configurez la copie du paquet de mise à jour dans le répertoire partagé dans les paramètres de Kaspersky Update Utility.

   Sélectionnez la source de mises à jour (par exemple, le stockage du Serveur d'administration) et le répertoire partagé dans lequel Kaspersky Update Utility va copier les paquets de mise à jour. Pour des informations détaillées sur l'utilisation de Kaspersky Update Utility, consultez la Base de connaissances Kaspersky.

3. Configurez la mise à jour des bases de données et des modules de l'application à partir du répertoire partagé spécifié sur d'autres appareils du réseau local de l'organisation : dans les `Update` paramètres de la tâche, définissez `SourceType=Custom` et indiquez le chemin d'accès au répertoire partagé dans la section `[Sources.item_#]`.

   L'adresse de la source des mises à jour doit correspondre à l'adresse renseignée dans les paramètres de Kaspersky Update Utility.

Procédure d'annulation des mises à jour des bases de données et des modules de l'application

Après la deuxième mise à jour des bases et modules d'application, la fonction de restauration des bases et modules d'application vers leurs versions précédentes devient disponible.

Chaque fois que l'utilisateur lance la mise à jour, Kaspersky Endpoint Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Ceci permet de revenir, le cas échéant, à l'utilisation des bases et des modules de l'application antérieurs. Il peut être utile de revenir à une version antérieure, par exemple si une nouvelle version de la base de données provoque un faux positif qui amène Kaspersky Endpoint Security à bloquer une application inoffensive.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, la tâche ne peut pas être utilisée pour annuler les mises à jour des bases de données.

Dans Kaspersky Security Center, vous pouvez créer des tâches d'annulation des mises à jour pour des groupes d'administration ou des appareils individuels à l'aide de Web Console ou de la Console d'administration.

Sur la ligne de commande, vous pouvez annuler une mise à jour des bases de données des manières suivantes :

- Exécutez la tâche prédéfinie *Annulation de la mise à jour des bases*.
- Créez et exécutez une tâche personnalisée *Annulation de la mise à jour des bases*.

La tâche *Annulation de la mise à jour des bases* n'a pas de paramètres.

Comment annuler une mise à jour des bases de données et des modules de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Retour en arrière**.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

   d. Sous **Appareils auxquels la tâche sera affectée**, sélectionnez la manière dont vous souhaitez définir la zone d'action de la tâche.

4. Sélectionnez les appareils selon la méthode de définition de la zone d'action de la tâche que vous préférez.

5. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Comment annuler une mise à jour des bases de données et des modules de l'application dans la Console d'administration

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez créer une tâche qui sera exécutée sur les appareils inclus dans le groupe d'administration sélectionné, dans l'arborescence de la console dans le dossier **Appareils administrés**, sélectionnez ce groupe d'administration, puis dans la zone de travail sélectionnez l'onglet **Tâches** et cliquez sur le bouton **Nouvelle tâche**.

     L'Assistant de création d'une tâche pour les appareils du groupe d'administration sélectionné démarre.

   - Si vous souhaitez créer une tâche qui sera exécutée sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console et cliquez sur le bouton **Nouvelle tâche** dans l'espace de travail.

     L'Assistant de création d'une tâche pour un ensemble d'appareils démarre.

2. À la première étape de l'Assistant, sélectionnez Kaspersky Endpoint Security dans la liste et le type de tâche **Annulation de la mise à jour des bases**.

3. Si vous créez une tâche pour un ensemble d'appareils, l'Assistant vous invite à sélectionner les appareils auxquels vous souhaitez attribuer la tâche. Sélectionnez la manière dont vous souhaitez définir la zone d'action de la tâche.

4. Sélectionnez les appareils selon la méthode de définition de la zone d'action de la tâche que vous préférez.

5. Configurez la planification de la tâche.

6. Saisissez le nom de la nouvelle tâche.

7. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

8. Dans la liste des tâches, sélectionnez la tâche, ouvrez le menu contextuel de la tâche et sélectionnez **Démarrer**.

Comment annuler une mise à jour des bases de données et des modules de l'application sur la ligne de commande

Exécutez la commande :

```
Annuler les mises à jour des bases et modules d'application
```

```
kesl-control --start-task 7
```

Comment annuler une mise à jour des bases de données et des modules de l'application dans l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour**.

   La fenêtre **Mise à jour** s'ouvre.

3. Cliquez sur le lien **Annuler la mise à jour** pour annuler la mise à jour des bases de données.

Protection contre les menaces contre l'hôte

Protection contre les fichiers malicieux

La Protection contre les fichiers malicieux offre un niveau minimal de sécurité à l'ordinateur. Le module est lancé avec Kaspersky Endpoint Security et analyse les fichiers en temps réel.

Fonctionnement de la Protection contre les fichiers malicieux

1. **L'application intercepte les événements liés aux opérations sur les fichiers et bloque les actions jusqu'à la fin de l'analyse.**

   L'application utilise un mécanisme d'interception des opérations sur les fichiers et bloque tout accès au fichier jusqu'à la fin de l'analyse.

2. **L'application analyse le fichier**

La Protection contre les fichiers malicieux analyse un fichier à l'aide des technologies suivantes :

- Bases antivirus.
- Services cloud de Kaspersky Security Network.
- La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

3. **Fin de l'analyse**

   Après l'analyse, l'application autorise l'opération ou la bloque et exécute l'action définie lors de la détection d'une menace.

Configuration initiale de la Protection contre les fichiers malicieux

La configuration initiale inclut les étapes nécessaires à la protection de base des terminaux.

1. **Sélection d'un mécanisme d'interception des événements système**

   La Protection contre les fichiers malicieux intercepte les événements liés aux opérations sur les fichiers et bloque les actions jusqu'à la fin de l'analyse.

   Lors de l'installation de l'application, vous avez sélectionné un mécanisme d'interception des événements système :

   - Mécanisme d'interception basé sur un module de noyau mis à jour
   - Mécanisme d'interception des événements système basé sur fanotify
   - Module de noyau pour la Protection contre les fichiers malicieux sur un système d'exploitation sans fanotify

   Le choix du mécanisme d'interception des événements système dépend de la configuration de l'ordinateur. La technologie d'interception qui offre les meilleures performances est celle du module de noyau mis à jour. Vous pouvez activer ce mécanisme dans les paramètres de l'application.

2. **Configurer la Protection contre les fichiers malicieux**

   Par défaut, la Protection contre les fichiers malicieux est activée et fonctionne avec les paramètres recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources. Si vous avez des exigences particulières en matière de sécurité de l'infrastructure, vous pouvez modifier ces paramètres.

3. **Configurer la zone de protection**

   Par défaut, l'application analyse tous les fichiers d'un appareil protégé. Si vous devez analyser uniquement un répertoire spécifique (par exemple, le répertoire dans lequel les fichiers sont automatiquement téléchargés depuis une source externe), vous pouvez définir uniquement ce répertoire comme zone de protection. Dans les autres cas, nous vous recommandons de conserver la zone de protection par défaut et d'utiliser des exclusions pour affiner cette zone.

4. **Exclure les points de montage de l'analyse**

   L'exclusion des points de montage pour l'analyse permet de ne pas intercepter les opérations sur les fichiers dans un répertoire donné. Par exemple, vous pouvez exclure les ressources réseau partagées de l'analyse et utiliser Kaspersky Endpoint Security pour les protéger sur l'appareil où ces ressources sont physiquement stockées. Vous pouvez également consulter les Recommandations pour la Protection contre les fichiers malicieux et les tâches d'analyse.

5. **Ajouter des exclusions**

   Les exclusions contribuent à maintenir un équilibre entre la sécurité et les performances du système. Pour garantir le fonctionnement stable des logiciels tiers, ajoutez aux exclusions les fichiers et les répertoires répertoriés dans la documentation du logiciel correspondant.

   Nous vous recommandons d'exclure les objets suivants :

   - Bases de données. L'analyse des bases de données volumineuses nécessite beaucoup de ressources. L'accès fréquent aux fichiers de bases de données déclenche des analyses fréquentes.
   - Fichiers utilisés par des processus gourmands en ressources. L'analyse de ces fichiers ralentit l'ordinateur.
   - Répertoires contenant des fichiers journaux. Le système d'exploitation écrit en permanence dans le fichier journal. Par conséquent, la Protection contre les fichiers malicieux consomme inutilement des ressources de l'ordinateur en analysant les journaux.

   Si un objet est exclu de l'analyse par le module Protection contre les fichiers malicieux, nous vous recommandons d'analyser ces objets à l'aide de la tâche *Analyse des logiciels malveillants*.

Configuration complémentaire pour les serveurs à forte charge

La configuration complémentaire comprend des étapes de réglage précis de la Protection contre les fichiers malicieux. Après la configuration initiale, si vous constatez des ralentissements ou si vous configurez des serveurs à forte charge, procédez comme suit :

1. **Désactiver le blocage de l'accès aux fichiers pendant les analyses**

   Par défaut, la Protection contre les fichiers malicieux bloque tout accès au fichier en cours d'analyse jusqu'à la fin de l'analyse. Si vous désactivez le mode de blocage, la Protection contre les fichiers malicieux fonctionne en mode d'information. Ce mode d'interception des opérations sur les fichiers a moins d'impact sur les performances du système, mais les menaces détectées dans les fichiers ne seront alors ni désinfectées ni supprimées. Vous pouvez exécuter la tâche Analyse des logiciels malveillants pour traiter ces menaces ultérieurement.

   Si le mode de blocage est désactivé, le Contrôle des appareils, l'action Prévention de l'exécution des objets et la tâche Analyse des disques amovibles fonctionnent également en mode d'information.

2. **Collecter les statistiques d'analyse des fichiers**

   Surveillez les principales mesures de performances de l'ordinateur : la charge du processeur, les performances des logiciels tiers ou d'autres indicateurs. Cela vous aidera à déterminer comment réduire la charge sur le système.

   Vous pouvez obtenir les statistiques d'analyse des fichiers à l'aide des outils d'analyse des performances des applications. Vous pouvez également utiliser vos propres outils de surveillance.

3. **Optimiser les performances de l'application**

Après avoir analysé les informations recueillies, optimisez les performances de l'application :

- Ajouter des exclusions globales
- Ajouter des exclusions
- Optimiser les paramètres de l'application

4. **Activer le blocage de l'accès aux fichiers pendant les analyses**

   Activer le blocage de l'accès aux fichiers pendant les analyses. En cas de détection d'un objet infecté, l'application effectuera l'action sélectionnée.

Considérations particulières et limitations

- Si l'utilisateur root n'a pas accès à un fichier dans un répertoire distant monté sur l'appareil via le protocole NFS4, l'application bloque l'accès à ce fichier pour tous les utilisateurs.
- Si la Protection contre les fichiers malicieux et la Surveillance du conteneur sont activées, l'application analyse également tous les espaces de noms et conteneurs.

Comment créer une zone de protection

Une *zone de protection* est une liste de chemins d'accès aux objets que Kaspersky Endpoint Security analyse à la recherche de menaces. Par défaut, l'application analyse tous les fichiers d'un appareil protégé. Si vous devez analyser uniquement un répertoire particulier (par exemple, le répertoire dans lequel les fichiers sont automatiquement téléchargés depuis une source externe), vous pouvez définir ce répertoire comme zone de protection. Dans les autres cas, nous vous recommandons de conserver la zone de protection par défaut et d'utiliser des exclusions pour affiner cette zone.

Kaspersky Endpoint Security analyse les objets dans l'ordre dans lequel ils apparaissent dans la liste des objets. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

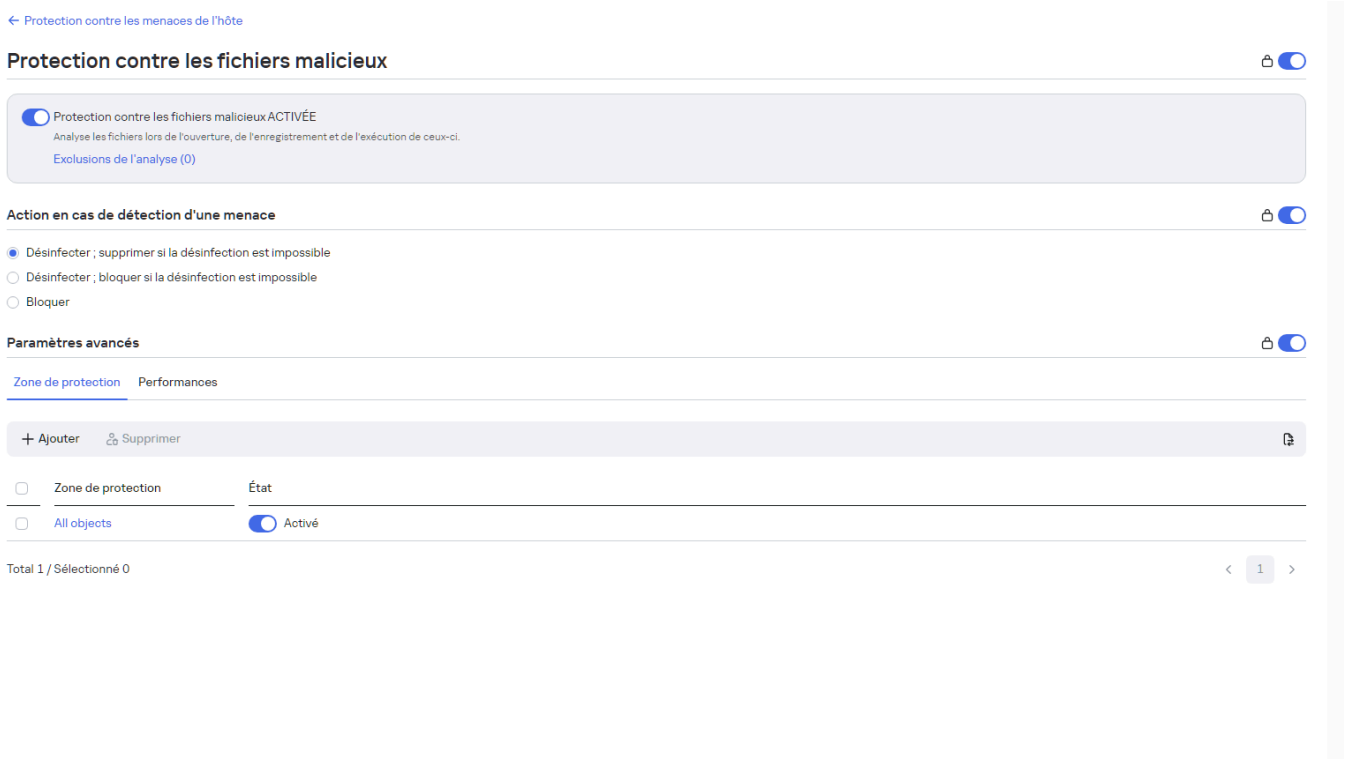
Comment créer une zone de protection dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Dans le groupe **Zone de protection**, cliquez sur **Ajouter**.
6. Une fenêtre s'ouvre ; dans celle-ci, sélectionnez le type de système de fichiers :
   - **Local**. Répertoires sur le disque dur accessibles sans connexion réseau.
   - **Monté**. Répertoires distants ou locaux montés.

- **Partagé**. Répertoires de l'ordinateur accessibles via les protocoles Samba (SMB) ou NFS.
- **Tous les systèmes montés distants**. Tous les répertoires distants montés sur l'appareil à l'aide des protocoles Samba et NFS.
- **Tous les éléments partagés**. Tous les répertoires de l'ordinateur accessibles via les protocoles Samba et NFS.

7. Pour un système de fichiers local, indiquez le chemin d'accès à un répertoire (par exemple, `/path/to/folder`). Le cas échéant, cochez la case **Inclure les sous-dossiers**.
8. Spécifiez le protocole d'accès à un système de fichiers monté ou partagé.
9. Spécifiez les masques des extensions d'objet (par exemple, `*.txt`). Séparez les masques par des virgules.
10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection contre les fichiers malicieux

Comment créer une zone de protection via la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 1 --add-path <path>
```

Une nouvelle section `[ScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application analyse les objets situés dans le répertoire défini par le paramètre `Path`.

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 1
```

Exemple

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Les paramètres suivants de la zone de protection sont ajoutés à la tâche :

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Comment sélectionner une action lors de la détection d'une menace dans un fichier

Lorsqu'une application malveillante est détectée, Kaspersky Endpoint Security peut supprimer le fichier infecté et mettre fin au processus malveillant lancé à partir de ce fichier. Dans les paramètres de la Protection contre les fichiers malicieux, vous pouvez sélectionner l'action que Kaspersky Endpoint Security exécute lorsqu'une menace est détectée.

Comment configurer l'action lors de la détection d'une menace dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Sous **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera en cas de détection d'une menace :

   - **Désinfecter ; supprimer si la désinfection est impossible** (par défaut). Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.
   - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier.
   - **Bloquer**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer l'action lors de la détection d'une menace depuis la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 1
```

Symboles

Options de la commande

Paramètre	Description
`ActionOnThreat`	Action lors de la détection d'une menace : • `DisinfectDeleteIfNotPossible` (par défaut). Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. • `DisinfectBlockIfNotPossible`. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier. • `Block`. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.

Qu'est-ce que le mode intelligent d'analyse des fichiers

La Protection contre les fichiers malicieux analyse tous les fichiers ouverts, enregistrés ou exécutés. Par défaut, la Protection contre les fichiers malicieux analyse les fichiers en mode intelligent. En *mode intelligent*, la Protection contre les fichiers malicieux analyse un fichier lors d'une tentative d'ouverture. Si un processus accède plusieurs fois à un fichier pendant une période donnée et le modifie, la Protection contre les fichiers malicieux n'analyse de nouveau le fichier que lorsque ce processus le ferme. Cela réduit au minimum l'impact de l'application sur les performances du système tout en offrant un niveau de protection élevé.

Pour que le mode intelligent fonctionne, le module de noyau mis à jour doit être sélectionné et lancé.

Vous ne pouvez pas modifier le mode d'analyse des fichiers dans Web Console.

Comment sélectionner le mode d'analyse des fichiers en ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 1
```

Symboles

Paramètre	Description
`ScanByAccessType`	Mode d'analyse des fichiers : • `SmartCheck` (valeur par défaut). La Protection contre les fichiers malicieux analyse les fichiers en mode intelligent. Kaspersky Endpoint Security analyse un fichier à son ouverture et à sa fermeture, s'il a été modifié. Si le mode intelligent n'est pas disponible, l'application analyse les fichiers à leur ouverture et chaque fois que le fichier est modifié (`OpenAndModify`). Le mode intelligent peut ne pas être disponible, par exemple si le module de noyau mis à jour est arrêté. • `OpenAndModify`. Kaspersky Endpoint Security analyse un fichier à son ouverture et chaque fois qu'il est modifié, et pas uniquement à sa fermeture. • `Open`. Kaspersky Endpoint Security analyse un fichier en cas de tentative d'ouverture de celui-ci pour lecture, exécution ou modification.

Comment optimiser l'analyse des fichiers

Configurez l'analyse des fichiers pour optimiser le module Protection contre les fichiers malicieux. Cela permet de réduire l'utilisation du processeur sur l'appareil protégé. Vous pouvez limiter l'analyse des archives, définir la taille maximale des objets pouvant être analysés et définir la durée maximale de l'analyse des objets.

Comment configurer l'analyse des fichiers dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Sous **Paramètres avancés**, sélectionnez l'onglet **Performances** et configurez l'analyse des fichiers :

   - **Analyser les archives**. Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). L'analyse est désactivée par défaut.
   - **Analyser les paquets de distribution et les archives auto-extractibles**. Analyse des paquets d'installation des applications tierces et des archives autoextractibles. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. L'analyse est désactivée par défaut.
   - **Analyser les bases de messagerie**. Analyse des bases de données de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres clients de messagerie. L'analyse est désactivée par défaut.
   - **Analyser les fichiers au format de messagerie**. Analyse des messages électroniques au format texte brut. L'analyse est désactivée par défaut.
   - **Ne pas analyser les archives de plus de (Mo)**. Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.
   - **Ignorer un fichier si son analyse prend plus de (secondes)**. Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre. Par défaut, l'application tente d'analyser un objet dans un délai d'une minute.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer l'analyse des fichiers en ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 1
```

Symboles

Options de la commande

Paramètre	Description
`ScanArchived`	Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). L'analyse est désactivée par défaut.
`ScanSfxArchived`	Analyse des paquets d'installation des applications tierces et des archives autoextractibles. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. L'analyse est désactivée par défaut.
`ScanMailBases`	Analyse des bases de données de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres clients de messagerie. L'analyse est désactivée par défaut.
`ScanPlainMail`	Analyse des messages électroniques au format texte brut. L'analyse est désactivée par défaut.
`SkipPlainTextFiles`	Exclusion temporaire de l'analyse des fichiers au format texte. L'application n'analyse pas les fichiers texte s'ils sont réutilisés par le même processus dans les 10 minutes suivant la dernière analyse. Par défaut, l'exclusion de l'analyse est désactivée. Ce paramètre est destiné aux appareils qui prennent en charge le mécanisme fanotify d'interception des événements système. Sur les appareils dotés du module de noyau mis à jour, l'application utilise le cache des résultats de l'analyse pour optimiser la charge.
`SkipDatabaseJournals`	Exclure temporairement les fichiers journaux de base de données de l'analyse. L'application n'analyse pas les fichiers journaux de base de données si le fichier journal est réutilisé par le même processus dans les 10 minutes suivant la dernière analyse. Par défaut, l'exclusion de l'analyse est désactivée. Ce paramètre est destiné aux appareils qui prennent en charge le mécanisme fanotify d'interception des événements système. Sur les appareils dotés du module de noyau mis à jour, l'application utilise le cache des résultats de l'analyse pour optimiser la charge.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse. (Valeur `0`).
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre. Par défaut, l'application tente d'analyser un objet dans un délai d'une minute. (Valeur `60`).

Particularités de l'analyse des liens symboliques et matériels

L'application Kaspersky Endpoint Security permet d'analyser les liens symboliques et matériels vers les fichiers.

Un *lien symbolique* (également appelé Soft link) est un fichier qui pointe vers un autre fichier ou répertoire. Un lien symbolique et le fichier vers lequel il pointe peuvent se trouver sur des systèmes de fichiers différents. De plus, un tel lien peut pointer vers un fichier qui n'existe pas. Lorsque vous supprimez le fichier cible, le lien n'est pas supprimé, mais il cesse de fonctionner.

Un *Hard link* est essentiellement un autre nom pour le fichier. Un lien matériel pointe vers le descripteur d'index (inode) du fichier qui contient les métadonnées du fichier. Tant qu'il reste au moins un lien matériel vers le fichier, le fichier continue d'exister dans le système de fichiers.

Analyse des liens symboliques

L'application analyse les liens symboliques uniquement si le fichier vers lequel le lien symbolique pointe se trouve dans la zone de protection de la Protection contre les fichiers malicieux.

Si le fichier se trouve en dehors de la zone de protection, l'application ne suit pas le lien symbolique pour analyser le contenu du fichier. Toutefois, si un tel fichier contient un code malveillant, la sécurité de l'appareil est menacée.

Analyse des liens matériels

Si un code malveillant est détecté dans un fichier vers lequel pointent plusieurs liens matériels, l'application désinfecte le fichier d'origine. Si la désinfection s'avère impossible, l'application supprime le lien matériel et crée à sa place une copie du fichier source portant le nom du lien supprimé dans la Sauvegarde. L'application supprime uniquement le lien matériel en cours de traitement ; les autres liens matériels susceptibles de pointer vers les mêmes données restent intacts.

Lorsque vous restaurez un lien matériel depuis la Sauvegarde, l'application crée à l'emplacement d'origine une copie du fichier d'origine portant le nom du lien matériel en cours de restauration. Le lien restauré ne devient pas un lien matériel vers le fichier d'origine et reste indépendant des autres liens matériels vers le même fichier.

Résolution des liens symboliques dans les exclusions par processus

Si le chemin indiqué dans le paramètre `ProgramPath` de la section `ExcludedForProgram` est un lien symbolique vers un fichier exécutable binaire, l'application applique l'exclusion au chemin du fichier cible. Cette règle s'applique à tous les liens vers ce fichier, et pas uniquement à celui indiqué explicitement. Ce paramètre utilise le chemin de l'image du programme. Par conséquent, les liens symboliques vers des scripts (par exemple, `.sh`) ne sont pas résolus.

Le fichier cible est déterminé lors de l'exécution de la tâche et de l'application des paramètres. Si un lien pointe vers un fichier inexistant, le chemin du lien lui-même est inclus dans les exclusions. Si le lien est remplacé par un fichier exécutable standard portant le même nom, l'exclusion s'appliquera à ce fichier.

Exemple d'exclusion avec un lien symbolique

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

Au moment du lancement de la tâche, le lien `/usr/bin/md5sum` pointe vers `/bin/coreutils`. Par conséquent, `/bin/coreutils` sera ajouté aux exclusions. Si le lien est ensuite redirigé vers `/bin/false`, l'exclusion continuera de s'appliquer à `/bin/coreutils` jusqu'au redémarrage de la tâche et ne s'appliquera pas à `/bin/false`. Après le redémarrage de la tâche, l'exclusion s'appliquera à `/bin/false` au lieu de `/bin/coreutils`.

Analyse des logiciels malveillants

L'analyse des logiciels malveillants est un élément important dans la protection de l'ordinateur. Elle doit être réalisée régulièrement pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de la protection en raison, par exemple, d'un niveau de sécurité faible ou pour toute autre raison.

Kaspersky Endpoint Security dispose de la tâche standard *Recherche d'applications malveillantes* prédéfinie. Vous pouvez utiliser cette tâche pour effectuer une analyse complète de l'appareil. Dans le cadre de la vérification complète, l'application analyse tous les objets sur les disques locaux de l'appareil, ainsi que tous les objets montés et communs, accessibles via les protocoles Samba et NFS, selon les paramètres de sécurité recommandés.

L'Assistant de configuration initiale du Serveur d'administration crée automatiquement une tâche *Recherche d'applications malveillantes*. Pour créer une tâche *Recherche d'applications malveillantes*, installez le plug-in d'administration de Kaspersky Endpoint Security for Linux pendant l'exécution de l'Assistant. Si nécessaire, vous pouvez créer des tâches définies par l'utilisateur du type *Recherche d'applications malveillantes*.

Paramètres de la tâche Recherche d'applications malveillantes

1. **Configurer le calendrier d'exécution de la tâche**

   Pendant l'analyse, Kaspersky Endpoint Security peut utiliser davantage de ressources de l'ordinateur que d'habitude. Nous recommandons de planifier les tâches d'analyse aux moments où l'ordinateur est le moins sollicité.

2. **Optimiser la charge imposée au système par l'analyse**

   Vous pouvez limiter l'utilisation du processeur lors de l'exécution de la tâche Analyse des logiciels malveillants. Il se peut alors que l'analyse de votre ordinateur prenne plus de temps.

   Kaspersky Endpoint Security permet d'annuler les tâches planifiées lorsqu'un ordinateur portable fonctionne sur batterie.

3. **Configurer les paramètres de la tâche Analyse des logiciels malveillants**

   Par défaut, la tâche Analyse des logiciels malveillants utilise les paramètres recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources. Si vous avez des exigences particulières en matière de sécurité de l'infrastructure, vous pouvez modifier ces paramètres.

   Par défaut, l'application analyse les archives. Pour ce faire, l'application décompresse les archives dans le répertoire /tmp. Assurez-vous que l'ordinateur dispose de suffisamment d'espace libre pour décompresser les archives.

4 Configurer la zone d'analyse

Par défaut, l'application analyse tous les fichiers d'un appareil protégé. Si vous devez analyser uniquement un répertoire particulier (par exemple, le répertoire dans lequel les fichiers sont automatiquement téléchargés depuis une source externe), vous pouvez indiquer uniquement ce répertoire comme zone d'analyse. Dans les autres cas, nous recommandons de conserver la zone d'analyse par défaut et d'utiliser des exclusions pour l'affiner.

Pour analyser les serveurs, nous recommandons de diviser la zone d'analyse en plusieurs sous-zones et de créer une tâche Analyse des logiciels malveillants distincte pour chacune de ces sous-zones. Pour répartir la charge, planifiez une heure de début différente pour chaque tâche.

5 Ajouter des exclusions de l'analyse

Configurer une zone d'exclusion :

- **Exclusions de l'analyse**. Les exclusions contribuent à maintenir un équilibre entre la sécurité et les performances du système. Pour assurer le fonctionnement stable des logiciels tiers, ajoutez aux exclusions les fichiers et répertoires répertoriés dans la documentation du logiciel concerné.

  Si vous avez déjà créé une zone d'exclusion pour le module Protection contre les fichiers malicieux, vous pouvez également appliquer ces exclusions à la tâche Analyse des logiciels malveillants.

- **Exclusions globales**. L'exclusion des points de montage (exclusions globales) permet de ne pas intercepter les opérations sur les fichiers dans certains répertoires. Excluez les ressources réseau partagées de la zone d'analyse. Pour protéger les ressources réseau partagées, utilisez l'application Kaspersky Endpoint Security sur l'appareil sur lequel les ressources sont physiquement stockées.

6 Lancer la tâche Analyse des logiciels malveillants

Comment lancer la tâche Analyse des logiciels malveillants dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche *Recherche d'applications malveillantes* pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Recherche d'applications malveillantes* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer une tâche *Recherche d'applications malveillantes*, installez le plug-in d'administration de Kaspersky Endpoint Security for Linux pendant l'exécution de l'Assistant.

   Si nécessaire, vous pouvez créer des tâches définies par l'utilisateur du type *Recherche d'applications malveillantes*.

3. Dans l'onglet **Paramètres**, gérez les paramètres de la tâche.

4. Dans l'onglet **Paramètres de l'application**, configurez les paramètres avancés de l'application (cf. tableau ci-après).

5. Dans l'onglet **Programmation**, configurez le mode de lancement de la tâche.

   Par défaut, Kaspersky Endpoint Security est configuré pour exécuter la tâche manuellement.

6. Enregistrez vos modifications.

7. Exécutez la tâche.

Paramètres de la tâche *Recherche d'applications malveillantes*

Paramètre	Description
Zone d'analyse	Un tableau contenant les zones vérifiées par la tâche. Par défaut, une seule zone d'analyse est active ; elle comprend tous les répertoires du système de fichiers local. Vous pouvez ajouter des zones d'analyse manuellement.
Action en cas de détection d'une menace	• **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.
Analyser les archives	Si cette option est activée, l'application analyse les archives. L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée de l'analyse des archives en spécifiant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ne pas analyser les fichiers de plus de (Mo)**. Cette option est désactivée par défaut.
Analyser les paquets de distribution et les archives auto-extractibles	Si cette option est activée, l'application analyse les archives autoextractibles. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Cette option est désactivée par défaut.
Analyser les fichiers au format de messagerie	Si cette option est activée, l'application analyse les messages électroniques au format texte. Cette fonction est désactivée par défaut.
Analyser les bases de messagerie	Si cette option est activée, l'application analyse les bases de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres applications de messagerie. Cette fonction est désactivée par défaut.
Ne pas analyser les fichiers de plus de (Mo)	Vous pouvez spécifier la taille maximale d'un fichier pouvant être analysé, en mégaoctets. Valeurs admises : 1 à 999999. Cette restriction est désactivée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Vous pouvez spécifier la durée maximale de l'analyse d'un fichier, en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 1 à 9999. Cette restriction est désactivée par défaut.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée. Cette fonction est désactivée par défaut.
Utiliser la technologie iChecker	Si cette option est activée, l'application analyse uniquement les nouveaux fichiers et les fichiers modifiés depuis la dernière analyse. Si cette option est désactivée, l'application analyse les fichiers sans tenir compte de leurs dates de création ou de modification. Cette option est désactivée par défaut.

Comment lancer la tâche Analyse des logiciels malveillants en ligne de commande

1. Par défaut, l'application dispose d'une tâche *Analyse des logiciels malveillants* (*Analyse_Mon_Ordinateur*). Si vous souhaitez créer une nouvelle tâche *Analyse des logiciels malveillants*, exécutez la commande suivante :

   ```
   kesl-control --create-task <task name> --type ODS
   ```

   où `<task name>` est le nom que vous souhaitez attribuer à la nouvelle tâche.

   Cette commande renvoie l'ID de la tâche créée.

2. Si nécessaire, modifiez les paramètres de la tâche (voir le tableau ci-dessous) à l'aide de la commande suivante :

   ```
   kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

   Exemple de modification des paramètres de la tâche

   ```
   kesl-control --set-settings 101 ScanFiles=No
   ```

   Vous pouvez également gérer les paramètres de la tâche à l'aide d'un fichier de configuration.

3. Si nécessaire, configurez une planification de la tâche. Par défaut, la tâche est lancée manuellement.

4. Pour vérifier les valeurs actuelles des paramètres de la tâche, exécutez la commande suivante :

   ```
   kesl-control --get-settings <task ID|name>
   ```

5. Pour lancer la tâche *Analyse des logiciels malveillants*, exécutez la commande suivante :

   ```
   kesl-control --start-task <task ID|name> [-W] [--progress]
   ```

   Exemples de commandes

   ```
   kesl-control --start-task 2 -W
   ```

6. Pour arrêter la tâche *Analyse des logiciels malveillants*, exécutez la commande suivante :

   ```
   kesl-control --stop-task <task ID|name> [-W]
   ```

Symboles

Paramètres de la tâche Analyse des logiciels malveillants

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fichiers. `No` : ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.

Paramètre	Description	Valeurs
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Active l'analyse des self-extracting archives uniquement (archives qui contiennent un module d'extraction exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Active l'analyse des messages électroniques au format plain text.	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.

Paramètre	Description	Valeurs
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.

Paramètre	Description	Valeurs
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `<device name mask>` – Analyser les secteurs d'amorçage des appareils dont le nom correspond au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		

`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
		`Exemple`
		`AreaDesc="Mail bases scan"`

`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.

Paramètre	Description	Valeurs
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple `AreaMask.item_0000=*doc`
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<path to local directory>` – Analyser les objets dans le répertoire indiqué. Le chemin `/` est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des masques pour spécifier le chemin. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Comment exécuter la tâche Analyse des logiciels malveillants depuis l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Cliquez sur **Analyse**.

   La fenêtre **Analyse** s'ouvre.
3. Pour démarrer une tâche d'analyse, cliquez sur le bouton **Démarrer** situé sous la tâche d'analyse que vous voulez démarrer.

   La progression de la tâche d'analyse en cours s'affiche.
4. Pour arrêter une tâche d'analyse, cliquez sur le bouton **Arrêter** situé sous la tâche d'analyse que vous voulez arrêter.

   La tâche d'analyse s'arrête, et des informations sur les objets analysés et les menaces détectées s'affichent.
5. Pour afficher le rapport de la tâche d'analyse, cliquez sur le bouton **Afficher le rapport**.

Lorsqu'un objet infecté est détecté ou lorsqu'une tâche d'analyse est terminée, la notification correspondante s'affiche.

La fenêtre **Analyse** affiche également la progression et les résultats des tâches temporaires d'analyse des secteurs d'amorçage (*Scan_Boot_Sectors_{ID}*) et des tâches temporaires d'analyse personnalisée des fichiers (*Scan_File_{ID}*).

7 Collecter les statistiques d'analyse de l'ordinateur

Vous pouvez utiliser les rapports pour obtenir les statistiques d'analyse d'un ordinateur. Assurez-vous que la durée de l'analyse se trouve dans une plage acceptable. Vérifiez les objets détectés et, si ces objets sont de confiance, ajoutez-les aux exclusions.

Considérations particulières et limitations

- Si l'utilisateur root n'a pas accès à un répertoire distant monté sur l'appareil via le protocole NFSv4, l'application ignore ce fichier pendant l'analyse.
- Lors de l'exécution des tâches d'analyse, Kaspersky Endpoint Security peut désinfecter et supprimer les fichiers protégés contre toute modification : les fichiers avec les attributs immutable et append-only et les fichiers dans les répertoires avec les attributs immutable et append-only. La sauvegarde conserve des copies de ces fichiers créés avant traitement ou suppression. Vous pouvez restaurer des fichiers à partir de sauvegardes si nécessaire. Une fois les tâches d'analyse terminées, les attributs immuables et append-only des fichiers désinfectés ne sont pas enregistrés.
- Si l'utilisateur ou le service de surveillance redémarre l'application pendant l'analyse des logiciels malveillants, ou si l'ordinateur est redémarré pendant l'analyse, l'analyse est arrêtée. Au prochain lancement de l'analyse des logiciels malveillants, celle-ci reprend depuis le début.

Articles utiles

Que faire si votre appareil manque d'espace disque disponible

Comment créer une zone d'analyse

Une *zone d'analyse* est une liste de chemins d'accès aux objets que Kaspersky Endpoint Security analyse à la recherche de menaces. Par défaut, l'application analyse tous les fichiers d'un appareil protégé. Si vous devez analyser uniquement un répertoire particulier (par exemple, le répertoire dans lequel les fichiers sont automatiquement téléchargés depuis une source externe), vous pouvez définir ce répertoire comme zone d'analyse.

Kaspersky Endpoint Security analyse les objets dans l'ordre dans lequel ils apparaissent dans la liste des objets. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Sur les systèmes d'exploitation utilisant le système de fichiers parsecfs (Astra Linux Special Edition), il est recommandé d'ajouter les chemins de montage de ce système de fichiers aux exclusions d'analyse.

Comment créer une zone d'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Zone d'analyse**, cliquez sur **Ajouter**.

5. Dans la liste déroulante **Système de fichiers, protocole d'accès et chemin**, sélectionnez le type de système de fichiers :

   - **Local**. Répertoires sur le disque dur accessibles sans connexion réseau.
   - **Monté**. Répertoires distants ou locaux montés.
   - **Partagé**. Répertoires de l'ordinateur accessibles via les protocoles Samba (SMB) ou NFS.
   - **Tous les systèmes montés distants**. Tous les répertoires distants montés sur l'appareil à l'aide des protocoles Samba et NFS.
   - **Tous les éléments partagés**. Tous les répertoires de l'ordinateur accessibles via les protocoles Samba et NFS.

6. Pour les types de systèmes de fichiers **Monté** et **Partagé**, sélectionnez un protocole d'accès :

   - **NFS**. Répertoires distants montés sur l'appareil via le protocole NFS.
   - **Samba**. Répertoires distants montés sur l'appareil via le protocole Samba.
   - **Personnalisé**. Ressources du système de fichiers sur un appareil d'un type autre que NFS ou Samba (par exemple, `ext4` ou `parsecfs`).

7. Indiquez le chemin d'accès au répertoire ou un masque de chemin.

8. Si nécessaire, spécifiez les masques des noms d'objet (par exemple, `*.txt` ou `report_*`). Séparez les masques par des virgules.

9. Cliquez sur **Ajouter**.

   Le nouvel objet est ajouté à la zone d'analyse. Vous pouvez exclure un objet de la zone d'analyse sans le supprimer de la liste des objets. Pour ce faire, désactivez le bouton bascule en regard de l'objet.

10. Si nécessaire, activez ou désactivez les objets prédéfinis dans la zone d'analyse :

    - **Mémoire du noyau**. **Mémoire des processus en cours**.
    - **Processus en cours d'exécution et objets de lancement**.
    - **Secteurs d'amorçage**.
    - **Tous les disques durs**.
    - **Tous les disques réseau**.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment créer une zone d'analyse sur la ligne de commande

1. Exécutez la commande:

   ```
   kesl-control --set-settings 2 --add-path <path>
   ```

   Une nouvelle section `[ScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application analysera les objets dans le répertoire spécifié.

   Exemple

   ```
   kesl-control --set-settings 2 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
   ```

   Les paramètres suivants de la zone d'analyse seront ajoutés à la tâche :

   ```
   [ScanScope.item_0001]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=/home
   AreaMask.item_0000=*
   ```

2. Si vous souhaitez inclure dans la zone d'analyse des ressources provenant d'un système de fichiers monté d'un type spécifique autre que NFS ou Samba (par exemple `parsecfs`), spécifiez le type de système de fichiers dans le paramètre `Path` : Path=<type de système de fichiers>

   L'application analysera toutes les ressources du système de fichiers indiqué de l'appareil.

   Exemple

   ```
   kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
   ```

   Les paramètres suivants de la zone d'analyse seront ajoutés à la tâche :

   ```
   [ScanScope.item_0002]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=parsecfs
   AreaMask.item_0000=*
   ```

3. Pour vérifier les valeurs actuelles des paramètres de la tâche, exécutez la commande suivante :

   ```
   kesl-control --get-settings 2
   ```

Comment configurer une planification d'analyse

L'exécution de la tâche *Analyse des logiciels malveillants* peut augmenter l'utilisation des ressources de l'ordinateur. Pour réduire l'impact de Kaspersky Endpoint Security sur les performances des ordinateurs des utilisateurs lorsqu'ils sont utilisés activement, vous pouvez planifier l'exécution de la tâche au moment le plus opportun.

Par exemple, si les employés de votre entreprise ont des horaires fixes, vous pouvez configurer l'analyse de manière à ce qu'elle s'exécute la nuit ou le week-end. Si l'exécution de l'analyse est impossible pour une raison quelconque (par exemple, l'ordinateur est éteint à ce moment-là), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

Si vous ne parvenez pas à déterminer le calendrier optimal pour l'exécution d'une analyse informatique, vous pouvez lancer la tâche *Analyse des logiciels malveillants* non seulement à des moments précis, mais aussi en fonction de conditions spécifiques, telles que le lancement d'une application, le téléchargement de mises à jour dans le référentiel, la détection d'une attaque virale ou l'achèvement d'une autre tâche. Vous pouvez également utiliser la fonctionnalité Wake-on-LAN pour allumer des ordinateurs qui sont éteints peu de temps avant le démarrage de la tâche. Vous pouvez configurer l'exécution de l'analyse à l'aide de la fonctionnalité Wake-on-LAN uniquement pour la tâche *Analyse des logiciels malveillants* de Kaspersky Security Center. Il est impossible d'activer la fonctionnalité Wake-on-LAN pour analyser l'ordinateur dans l'interface de l'application.

Comment lancer la tâche Analyse des logiciels malveillants dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

4. Configurez la planification des tâches d'analyse.

5. En fonction de la fréquence sélectionnée, configurez les paramètres complémentaires afin d'affiner la planification du lancement de la tâche.

6. Enregistrez vos modifications.

Paramètres de planification de l'analyse

Paramètre	Description
Démarrer la tâche	**Mode manuel**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. Selon la planification. Le mode d'exécution de la tâche d'analyse où l'application exécute la tâche d'analyse selon la planification que vous avez créée. Si ce mode d'exécution de la tâche d'analyse est sélectionné, vous pouvez également lancer la tâche d'analyse manuellement.
Lancer les tâches non exécutées	Si la case est cochée, Kaspersky Endpoint Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Adopter un décalage aléatoire automatique pour les lancements de tâche	Si la case est cochée, la tâche n'est pas exécutée strictement selon la planification, mais de manière aléatoire dans un certain intervalle, c'est-à-dire que les heures de lancement de la tâche sont étalées. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. La plage des heures de lancement aléatoires est calculée automatiquement lors de la création de la tâche, en fonction du nombre d'ordinateurs auxquels la tâche est assignée. Par la suite, la tâche est toujours exécutée à son heure de lancement calculée. Toutefois, lorsque les paramètres de la tâche sont modifiés ou que la tâche est exécutée manuellement, l'heure de lancement calculée change. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche	Si la case est cochée, le système d'exploitation de l'ordinateur dispose d'un délai déterminé pour terminer le lancement avant l'exécution de la tâche. Le délai par défaut est de 5 minutes. Cochez la case si vous souhaitez exécuter la tâche sur tous les ordinateurs, y compris sur les ordinateurs éteints.

Paramètre	Description
Arrêter les appareils après la fin de la tâche	Si cette case est cochée, l'ordinateur s'éteint une fois la tâche terminée. Par exemple, vous pouvez activer cette fonctionnalité pour analyser l'ordinateur le vendredi après les heures de travail. Une fois la tâche terminée, l'application éteint l'ordinateur pour le week-end.
Arrêter la tâche si elle prend plus de	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

Planification de la tâche Analyse des logiciels malveillants via la ligne de commande

Pour exécuter la tâche une fois à un moment précis, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

Pour exécuter la tâche tous les mois, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

Pour exécuter la tâche un jour précis de la semaine, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

Pour exécuter la tâche à intervalles réguliers exprimés en jours, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

Pour exécuter la tâche à intervalles réguliers exprimés en heures à partir d'une date précise, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

Pour exécuter la tâche à intervalles réguliers à partir d'une date précise, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

Pour exécuter la tâche immédiatement après le démarrage de l'application, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=PS
```

Pour exécuter la tâche immédiatement après la mise à jour des bases de données, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=BR
```

Pour désactiver la planification de la tâche, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RuleType=Manual
```

Pour gérer les paramètres supplémentaires de planification de la tâche, exécutez la commande suivante :

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

Pour vérifier les valeurs actuelles des paramètres de la tâche, exécutez la commande suivante :

```
kesl-control --get-schedule 2
```

Symboles

Paramètres de la programmation du lancement d'une tâche

Paramètre	Description
`RuleType`	Planifier l'exécution de la tâche. • `Once` : exécuter la tâche une fois. • `Monthly` : exécuter la tâche chaque mois, le jour et l'heure spécifiés. • `Weekly` : exécuter la tâche chaque semaine, le jour et l'heure spécifiés. • `Daily` : exécuter la tâche régulièrement, avec un intervalle spécifié en jours. • `Hourly` : exécuter la tâche régulièrement, à un intervalle spécifié en heures, à partir de la date et de l'heure spécifiées. • `Minutely` : exécuter la tâche régulièrement, à un intervalle spécifié en minutes, à partir de l'heure spécifiée. • `Manual` : lance la tâche manuellement. • `PS` : lance la tâche après le lancement de l'application. • `BR` : lancement de la tâche après la mise à jour des bases de données de l'application.
`StartTime`	La date et l'heure du lancement de la tâche. Le format de ce paramètre dépend de `RuleType`. Valeurs possibles : • `<year>` : 1970 à 2099 • `<month>` : JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>` : 1 à 31 • `<day of the week>` : Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>` : 0 à 23 • `<mm>` : 0 à 59 • `<ss>` : 0 à 59 • `<interval between runs (in days)>` : 0 à 364 • `<interval between runs (in hours)>` : 0 à 23 • `<interval between runs (in minutes)>` : 0 à 59
`RandomInterval`	Exécutez la tâche sur les ordinateurs de manière aléatoire dans un intervalle de temps donné (de 0 à la valeur spécifiée). Cela évite le lancement simultané de plusieurs tâches. Valeur par défaut : 99 minutes. Valeurs possibles : 0 à 999.
`RunMissedStartRules`	Lancement d'une tâche ignorée après le lancement de l'application. • `Yes` (valeur par défaut) signifie que l'exécution d'une tâche non exécutée est activée. Si l'application est arrêtée ou si l'ordinateur est éteint alors qu'une tâche planifiée est en cours d'exécution, Kaspersky Endpoint Security lance cette tâche immédiatement après le démarrage de l'application. Cela vous permet de vous assurer que les tâches critiques ne sont jamais omises. • `No` signifie que l'exécution d'une tâche non exécutée est désactivée. Si l'application est arrêtée ou si l'ordinateur est éteint alors qu'une tâche planifiée est en cours d'exécution, l'application ignore cette tâche. Cela permet d'éviter une surcharge lors du lancement de l'application.
`UseWorkingTimeout`	Arrêt de la tâche lorsque la durée maximale d'exécution de la tâche spécifiée par le paramètre `WorkingTimeout` est atteinte. La tâche sera arrêtée même si elle n'est pas terminée. Le prochain lancement de la tâche sera effectué comme prévu. • `Yes` : arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte. • `No` (valeur par défaut) : ne pas arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte.

Paramètre	Description
`WorkingTimeout`	Le temps maximum d'exécution de la tâche (en minutes), après lequel l'application arrête l'exécution de la tâche, si la valeur du paramètre `UseWorkingTimeout=Yes`. Valeur par défaut : 120 minutes. Valeurs possibles : 1 à 999.

Exemple d'exécution de la tâche d'analyse toutes les 10 heures

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

Exemple d'exécution de la tâche d'analyse le 15 de chaque mois

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

Exemple d'exécution de la tâche tous les mardis

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

Analyse d'un fichier ou d'un répertoire individuel

Kaspersky Endpoint Security vous permet d'effectuer une analyse de fichiers individuels à la recherche de virus et autres applications malveillantes à l'aide de la ligne de commande. Par exemple, vous pouvez analyser de manière sélective les archives pour lesquelles l'analyse de la Protection contre les fichiers malicieux est désactivée par défaut.

Par défaut, l'application analyse le fichier à l'aide des paramètres de la tâche *Scan_File (ID : 3)* recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources. Par défaut, l'application enregistre une copie de l'objet infecté dans la Sauvegarde et tente de désinfecter l'objet. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. Vous pouvez sélectionner une autre action lors de la détection d'une menace et gérer les autres paramètres de la tâche.

Lancement de l'analyse d'un fichier ou d'un répertoire individuel via la ligne de commande

```
kesl-control --scan-file <path to the file or directory>
```

Par conséquent, Kaspersky Endpoint Security génère un rapport sous la forme suivante :

```
Objets analysés : N

Nombre total d'objets détectés : N

Objets infectés et autres objets : N

Objets désinfectés : N

Placé dans la sauvegarde : N

Objets supprimés : N

Objets non désinfectés : N

Erreurs d'analyse : N
```

```
Objets protégés par mot de passe : N

Objets ignorés : N

Détecté à l'aide de Cloud Sandbox : N
```

Optimisation des tâches d'analyse personnalisée

Pour optimiser les analyses personnalisées, vous pouvez limiter le lancement simultané de plusieurs tâches. Si un utilisateur tente d'exécuter trop de tâches d'analyse personnalisée en même temps, l'application n'exécute pas les tâches qui dépassent la limite. Cela vous permet de contrôler l'utilisation des ressources de l'appareil client et, par exemple, d'éviter une charge excessive sur le serveur. Par défaut, la limite du nombre de tâches d'analyse personnalisée est définie sur 100.

Kaspersky Endpoint Security limite les tâches uniquement pour les utilisateurs non privilégiés. Un utilisateur disposant de privilèges root peut exécuter des tâches d'analyse personnalisée sans limitation.

Vous pouvez configurer la limite du nombre de tâches d'analyse personnalisée en ligne de commande à l'aide des paramètres généraux de l'application. Vous ne pouvez pas configurer la limite du nombre de tâches dans la Console d'administration ou dans Web Console.

Optimisation des tâches d'analyse personnalisée en ligne de commande

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

Analyse des zones critiques

Une tâche d'analyse spéciale vous permet d'analyser uniquement les zones critiques de l'ordinateur : *Analyse des zones critiques*. La tâche *Analyse des zones critiques* analyse rapidement les zones de l'ordinateur où les applications malveillantes sont détectées le plus souvent. La zone d'analyse de cette tâche inclut les secteurs d'amorçage, les objets de démarrage, la mémoire du noyau et les processus en cours d'exécution.

Une application malveillante qui parvient à compromettre les zones critiques de l'ordinateur peut exécuter ses fonctions tout en échappant à la détection. Par défaut, l'application exécute la tâche avec les paramètres recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources.

Les experts de Kaspersky recommandent de ne pas modifier les paramètres par défaut de la tâche *Analyse des zones critiques*.

Si l'utilisateur root n'a pas accès à un répertoire distant monté sur l'appareil via le protocole NFSv4, l'application ignore ce fichier pendant l'analyse.

L'Assistant de configuration initiale du Serveur d'administration crée automatiquement une tâche *Analyse des zones critiques*. Pour créer une tâche *Analyse des zones critiques*, installez le plug-in d'administration de Kaspersky Endpoint Security for Linux pendant l'exécution de l'Assistant. Si nécessaire, vous pouvez créer des tâches définies par l'utilisateur du type *Analyse des zones critiques*.

Exécution d'une analyse des zones critiques dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Endpoint Security for Linux**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Analyse des zones critiques**.

   c. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple *Analyse des zones critiques après une infection de l'ordinateur*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Quittez l'Assistant.

6. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.

7. Sélectionnez l'onglet **Paramètres de l'application**.

8. Configurez la tâche d'analyse (cf. tableau ci-après).

9. Si nécessaire, configurez les paramètres de planification du lancement de la tâche sous l'onglet **Programmation**.

10. Enregistrez vos modifications.

11. Lancer la tâche de recherche de virus.

Paramètres de la tâche Analyse des zones critiques

Paramètre	Description
Zone d'analyse	Un tableau contenant les zones vérifiées par la tâche. Par défaut, la zone d'analyse inclut tous les répertoires du système de fichiers local, la mémoire du noyau, la mémoire des processus en cours d'exécution, les objets de démarrage et les secteurs d'amorçage.
Action en cas de détection d'une menace	• **Désinfecter ; supprimer si la désinfection est impossible** (par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Paramètre	Description
Analyser les archives	Si cette option est activée, l'application analyse les archives. L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée de l'analyse des archives en spécifiant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ne pas analyser les fichiers de plus de (Mo)**. Cette option est désactivée par défaut.
Analyser les paquets de distribution et les archives auto-extractibles	Si cette option est activée, l'application analyse les archives autoextractibles. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Cette option est désactivée par défaut.
Analyser les fichiers au format de messagerie	Analyse des messages électroniques au format texte brut. Cette fonction est désactivée par défaut.
Analyser les bases de messagerie	Si cette option est activée, l'application analyse les bases de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres applications de messagerie. Cette fonction est désactivée par défaut.
Ne pas analyser les fichiers de plus de (Mo)	Vous pouvez spécifier la taille maximale d'un fichier pouvant être analysé, en mégaoctets. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Cette fonction est désactivée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Vous pouvez spécifier la durée maximale de l'analyse d'un fichier, en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Cette fonction est désactivée par défaut.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée. Cette fonction est désactivée par défaut.
Utiliser la technologie iChecker	Si cette option est activée, l'application analyse uniquement les nouveaux fichiers et les fichiers modifiés depuis la dernière analyse. Si cette option est désactivée, l'application analyse les fichiers sans tenir compte de leurs dates de création ou de modification. Cette option est désactivée par défaut.

Comment exécuter la tâche d'analyse des zones critiques en ligne de commande

1. Si nécessaire, configurez les paramètres de la tâche (voir le tableau ci-dessous).

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. Si nécessaire, configurez la planification de la tâche.

3. Pour vérifier les valeurs actuelles des paramètres de la tâche, exécutez la commande suivante :

```
kesl-control --get-settings 4 [--json]
```

où `--json` : afficher les données au format JSON.

4. Pour lancer la tâche, exécutez la commande suivante :

```
kesl-control --start-task 4 [-W] [--progress]
```

Où :

- `[-W]` active la sortie des événements actuels liés à la tâche.
- `[--progress]` : afficher la progression de la tâche.

Si nécessaire, vous pouvez créer des tâches définies par l'utilisateur de type *Analyse des zones critiques*.

Paramètres de la tâche Analyse des zones critiques

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` : analyse les fichiers. `No` (valeur par défaut) — Ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Active l'analyse des self-extracting archives uniquement (archives qui contiennent un module d'extraction exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Active l'analyse des messages électroniques au format plain text.	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.

Paramètre	Description	Valeurs
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

Paramètre	Description	Valeurs

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.

Paramètre	Description	Valeurs
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `<device name mask>` – Analyser les secteurs d'amorçage des appareils dont le nom correspond au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section `[ScanScope.item_#]` contient les paramètres suivants :		

`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
		`Exemple`
		`AreaDesc="Mail bases scan"`

`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.

`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell.
	Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.
		Valeur par défaut : `*` (analyser tous les objets).
		`Exemple`
		`AreaMask.item_<item number>=*doc`

`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<path to local directory>` – Analyser les objets dans le répertoire indiqué. Le chemin `/` est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section `[ExcludedFromScanScope.item_#]` contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des masques pour spécifier le chemin. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Analyser les conteneurs

Kaspersky Endpoint Security peut analyser les conteneurs et les images à la recherche d'applications malveillantes en temps réel ou à la demande.

Pour utiliser les fonctionnalités d'analyse du conteneur, vous avez besoin d'une licence incluant cette fonctionnalité.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Surveillance des conteneurs

Le module *Surveillance des conteneurs* analyse les conteneurs et les espaces de noms en cours d'exécution en temps réel. Par défaut, le module Surveillance du conteneur est activé.

Pour que le module Surveillance du conteneur fonctionne, le module Protection contre les fichiers malicieux doit être activé. Les paramètres du module Protection contre les fichiers malicieux sont appliqués lors de l'analyse des conteneurs et des espaces de noms.

Le scénario recommandé de configuration de la Surveillance des conteneurs comprend les étapes suivantes :

1. **Configurez l'intégration de l'application avec les outils de gestion des conteneurs**

   L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc.

2. **Créer une zone de protection**

   Déterminez les appareils sur lesquels vous souhaitez analyser les conteneurs et les espaces de noms.

3. **Dans les paramètres de la Surveillance des conteneurs, sélectionnez l'action Ignorer le conteneur**

   Lorsqu'un objet infecté est détecté dans un conteneur, Kaspersky Endpoint Security peut arrêter immédiatement le conteneur, ne rien faire ou arrêter le conteneur si la désinfection de l'objet ou l'élimination de la menace s'est avérée impossible. Sélectionnez l'action **Ignorer le conteneur** pour tester le module. L'application n'exécutera aucune action sur le conteneur lorsqu'un objet infecté est détecté, mais consignera les informations relatives aux menaces détectées.

4. **Collecter les statistiques de la Surveillance des conteneurs**

   Vous pouvez obtenir les statistiques de la Surveillance des conteneurs à l'aide de rapports.

5. **Sélectionnez l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté.**

   Sélectionner l'action que l'application effectuera sur le conteneur lorsqu'un objet infecté est détecté.

Analyse à la demande des conteneurs

L'application peut analyser à la demande les conteneurs et les images à la recherche de virus et d'autres applications malveillantes. Cette opération est effectuée à l'aide de la tâche prédéfinie *Analyse du conteneur (Container_Scan)*. Vous pouvez configurer la tâche prédéfinie ou créer des tâches définies par l'utilisateur pour analyser les conteneurs via la ligne de commande, dans Web Console ou dans la Console d'administration.

Une application peut effectuer simultanément plusieurs tâches d'analyse du conteneur.

Le scénario recommandé de configuration de l'Analyse du conteneur comprend les étapes suivantes :

1. **Configurez l'intégration de l'application avec les outils de gestion des conteneurs**

   L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc.

2. **Configurer une zone d'analyse**

   Par défaut, l'application analyse tous les conteneurs sur un appareil protégé. Si vous devez analyser uniquement des conteneurs individuels, vous pouvez spécifier leurs noms ou des masques de nom.

3. **Dans les paramètres de l'Analyse du conteneur, sélectionnez les actions Ignorer le conteneur et Ignorer l'image**

   Lorsqu'un objet infecté est détecté dans un conteneur, Kaspersky Endpoint Security peut arrêter immédiatement le conteneur, ne rien faire ou arrêter le conteneur si la désinfection de l'objet ou l'élimination de la menace s'est avérée impossible. Si un objet infecté est détecté dans l'image du conteneur, Kaspersky Endpoint Security peut supprimer l'image du conteneur ou n'exécuter aucune action sur celle-ci. Sélectionnez les actions **Ignorer le conteneur** et **Ignorer l'image** pour tester la tâche. Lorsqu'un objet infecté est détecté, l'application n'exécutera aucune action sur le conteneur ni sur l'image, mais consignera les informations relatives aux menaces détectées.

4. **Collecter les statistiques de l'Analyse du conteneur**

   Vous pouvez obtenir les statistiques de l'Analyse du conteneur à l'aide des rapports.

5. **Optimiser les performances de l'application**

   Après avoir analysé les informations recueillies, optimisez les performances de l'application :

   - Ajouter des exclusions globales
   - Ajouter des exclusions de l'analyse
   - Optimiser l'Analyse du conteneur

6. **Sélectionnez l'action à effectuer sur un conteneur et son image lorsqu'un objet infecté est détecté**

   Sélectionnez les actions que l'application effectue sur un conteneur et son image lorsqu'elle détecte un objet infecté.

Analyse personnalisée du conteneur

La tâche *Analyse personnalisée du conteneur* permet de configurer et d'enregistrer les paramètres utilisés lors de l'analyse des conteneurs et des images spécifiés à l'aide de la commande suivante :

```
kesl-control --scan-container
```

Une analyse personnalisée est effectuée avec les paramètres stockés dans la tâche prédéfinie *Custom_Container_Scan* (ID:19). Vous pouvez configurer les paramètres de l'analyse personnalisée du conteneur et des images en modifiant les paramètres de cette tâche. Par défaut, la tâche *Custom_Container_Scan* a les mêmes paramètres que la tâche *Container_Scan* (ID:18).

La commande crée et exécute une tâche temporaire d'analyse des conteneurs et des images, laquelle est automatiquement supprimée une fois terminée. Parallèlement, les résultats de l'analyse sont affichés dans la console.

Considérations particulières et limitations

- L'application ne vérifie pas les espaces de noms et les conteneurs à moins que les modules permettant de travailler avec les conteneurs et les espaces de noms ne soient installés sur le système d'exploitation. Dans ce cas, l'état du module Surveillance du conteneur sur la ligne de commande est affiché comme « La tâche est disponible et n'est pas en cours d'exécution », tandis que dans Kaspersky Security Center, il est affiché comme « Arrêtée ».
- Une action de Surveillance du conteneur ne peut être sélectionnée que si la licence de l'application inclut cette fonction.

Configuration de l'intégration avec les outils de gestion des conteneurs

L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc. Vous pouvez configurer l'intégration avec ces outils de gestion des conteneurs.

Comment configurer l'intégration avec les outils de gestion des conteneurs dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Paramètres généraux** → **Paramètres d'analyse du conteneur**.
5. Assurez-vous que le bouton bascule du module Surveillance des conteneurs se trouve en position **Surveillance des espaces de noms et des conteneurs ACTIVÉE**.
6. Cliquez sur le bouton **Configurer** dans le groupe **Paramètres d'analyse du conteneur**.

7. La fenêtre **Paramètres d'analyse** s'ouvre ; dans cette fenêtre, cochez les cases en regard des outils de gestion des conteneurs installés et utilisés dans le système d'exploitation des appareils protégés, puis gérez les paramètres si nécessaire :

   - La case à cocher **Utiliser Docker** active le système de gestion des conteneurs Docker. La case est cochée par défaut.

     - Le champ **Chemin d'accès au socket Docker** permet de saisir le chemin d'accès ou l'URI (identificateur uniforme de ressource) du socket Docker. Valeur par défaut : /var/run/docker.sock.

   - La case à cocher **Utiliser CRI-O** active l'environnement CRI-O. La case est cochée par défaut.

     - Le champ **Chemin d'accès au fichier** permet de saisir le chemin d'accès au fichier de configuration CRI-O. Valeur par défaut : /etc/crio/crio.conf.

   - La case à cocher **Utiliser Podman** active l'utilitaire Podman. La case est cochée par défaut.

     - Le champ **Chemin d'accès au fichier** permet de saisir le chemin d'accès au fichier exécutable de l'utilitaire Podman. Valeur par défaut : /usr/bin/podman.

     - Le champ **Répertoire racine** permet de saisir le chemin d'accès au répertoire racine du stockage des conteneurs.

   - La case à cocher **Utiliser runc** active l'utilitaire runc. La case est cochée par défaut.

     - Le champ **Chemin d'accès au fichier** permet de saisir le chemin d'accès au fichier exécutable de l'utilitaire runc. Valeur par défaut : /usr/bin/runc.

     - Le champ **Répertoire racine** permet de saisir le chemin d'accès au répertoire racine du stockage de l'état des conteneurs. Valeur par défaut : /run/runc.

8. Enregistrez vos modifications.

Comment configurer l'intégration avec les outils de gestion des conteneurs sur la ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver la surveillance en temps réel des espaces de noms et des conteneurs à l'aide du paramètre `NamespaceMonitoring=<Yes|No>` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre `NamespaceMonitoring` à l'aide du fichier de configuration, qui contient tous les paramètres généraux de l'application, ou à l'aide des clés de la ligne de commande.

Activer la surveillance des espaces de noms et des conteneurs à l'aide des options de ligne de commande

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

Lors de l'analyse en temps réel des espaces de noms et des conteneurs, les paramètres de l'analyse du conteneur sont appliqués. Vous pouvez afficher et modifier ces paramètres à l'aide des commandes spéciales de gestion de Kaspersky Endpoint Security :

- Vous pouvez afficher les valeurs actuelles des paramètres de l'analyse du conteneur dans la console ou dans un fichier de configuration. Vous pouvez utiliser ce fichier pour modifier les paramètres.
- Vous pouvez modifier tous les paramètres de l'analyse du conteneur à l'aide du fichier de configuration contenant les paramètres. Vous pouvez obtenir le fichier de configuration à l'aide de la commande pour afficher les paramètres généraux de l'analyse du conteneur.
- Vous pouvez gérer des paramètres individuels à l'aide d'options de ligne de commande au format `<setting name>=<setting value>`. Vous pouvez obtenir les valeurs actuelles des paramètres à l'aide d'une commande permettant d'afficher les paramètres de l'analyse du conteneur.

Afficher les valeurs actuelles des paramètres de l'analyse du conteneur dans la console

```
kesl-control --get-container-settings [--json]
```

Où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Exporter les valeurs actuelles des paramètres de l'analyse du conteneur dans un fichier

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

Où :

- `--file <path to configuration file>` est le chemin d'accès au fichier dans lequel vous voulez enregistrer les paramètres de l'analyse du conteneur. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour modifier les valeurs des paramètres de l'analyse du conteneur à l'aide d'un fichier de configuration :

1. Exportez les paramètres de l'analyse du conteneur dans un fichier de configuration, comme décrit ci-dessus.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande:

   ```
   kesl-control --set-container-settings --file <path to configuration file> [--json]
   ```

   Où :

   - `--file <path to configuration file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres de l'analyse du conteneur.
   - `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de l'analyse du conteneur spécifiées dans le fichier sont importées dans l'application.

Modifier les valeurs des paramètres de l'analyse du conteneur à l'aide des options de ligne de commande

```
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Où `<setting name>=<setting value>` correspond au nom et à la valeur d'un paramètre de l'analyse du conteneur.

Les valeurs des paramètres spécifiés de l'analyse du conteneur sont modifiées.

Création d'une zone d'analyse à la demande pour les conteneurs et les images

Zone d'analyse

Une *zone d'analyse* est une liste de noms de conteneurs que Kaspersky Endpoint Security analyse lors de l'exécution de la tâche *Analyse du conteneur*.

Par défaut, la tâche *Analyse du conteneur* analyse tous les conteneurs sur un appareil protégé. Si vous devez analyser uniquement des conteneurs individuels, vous pouvez spécifier leurs noms ou des masques de nom.

Comment créer une zone d'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Dans la liste des tâches, sélectionnez la tâche Analyse du conteneur de Kaspersky Endpoint Security et cliquez sur le nom de la tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sous **Paramètres d'analyse avancés** → **Paramètres d'analyse du conteneur**, dans le champ **Masque de nom**, saisissez le nom ou le masque de nom du conteneur que vous souhaitez analyser. Par défaut, tous les conteneurs sont analysés.

5. Sous **Paramètres d'analyse avancés** → **Paramètres d'analyse d'image**, dans le champ **Masque de nom**, saisissez le nom ou le masque de nom de l'image de conteneur que vous souhaitez analyser. Par défaut, toutes les images sont analysées.

6. Enregistrez vos modifications.

Comment créer une zone d'analyse sur la ligne de commande

1. Configurez une zone d'analyse à l'aide de la commande suivante :

   ```
   kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
   ScanImages=Yes ImageNameMask=<image name or mask>
   ```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

- `<container name or mask>` est le nom ou le masque de nom du conteneur que vous souhaitez analyser. Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères `?` et `*`. Par défaut, tous les conteneurs sont analysés.

- `<image name or mask>` est le nom ou le masque de nom de l'image que vous souhaitez analyser. Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères `?` et `*`. Par défaut, toutes les images sont analysées.

2. Vous pouvez également configurer une zone d'analyse à l'aide d'un fichier de configuration :

   a. Exportez les paramètres de la tâche dans un fichier de configuration en exécutant la commande suivante :

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Ouvrez le fichier de configuration afin de le modifier.

   c. Ajoutez les paramètres suivants au fichier :

   - `ScanContainers=Yes` active l'analyse des conteneurs spécifiés.

   - `ContainerNameMask=<container name or mask>` est le nom ou le masque de nom du conteneur que vous souhaitez analyser. Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères `?` et `*`. Par défaut, tous les conteneurs sont analysés.

- `ScanImages=Yes` active l'analyse des images spécifiées.
- `ImageNameMask=<image name or mask>` est le nom ou le masque de nom de l'image que vous souhaitez analyser. Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères `?` et `*`. Par défaut, toutes les images sont analysées.

Exemple d'analyse d'un conteneur effectuée sur un conteneur nommé my_container

```
ContainerNameMask=my_container
```

Exemple d'analyse de tous les conteneurs dont les noms commencent par my_container

```
ContainerNameMask=my_container*
```

Exemple d'analyse de conteneur effectuée sur tous les conteneurs dont les noms commencent par my_, puis contiennent cinq caractères quelconques, puis _container et se terminent par une séquence quelconque de caractères

```
ContainerNameMask=my_?????_container*
```

Exemple d'analyse d'images effectuée sur des images portant le nom "my_image" et le tag "latest"

```
ImageNameMask=my_image:latest
```

Exemple d'analyse d'images effectuée sur toutes les images dont les noms commencent par my_image_ et avec n'importe quel tag

```
ImageNameMask=my_image*
```

d. Enregistrez les modifications dans le fichier de configuration.

e. Importez les paramètres du fichier de configuration dans la tâche à l'aide de la commande suivante :

```
kesl- <task ID|name> --file <path> [--json]
```

Où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--file <path>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si l'option --json n'est pas spécifiée, l'application tente d'importer depuis un fichier INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de la tâche définies dans le fichier seront importées dans l'application.

Exclusions de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux. Les exclusions d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky.

Vous pouvez également exclure certains répertoires de confiance de la zone d'analyse afin d'optimiser les performances de l'application.

Vous pouvez exclure de l'analyse des objets à l'aide des méthodes suivantes :

- **Exclusions par masque**. Saisissez un nom de fichier avec un masque. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

  Utilisez des masques :

  - Le caractère `*` (astérisque), qui remplace n'importe quelle suite de caractères, à l'exception des caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/*/*.txt` inclura tous les chemins d'accès aux fichiers portant l'extension TXT situés dans des répertoires du répertoire dir, mais pas dans des sous-répertoires.

  - Deux caractères `*` consécutifs remplacent n'importe quelle suite de caractères (y compris une suite vide) dans le nom de fichier ou de répertoire, y compris les caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/**/*.txt` inclura tous les chemins d'accès aux fichiers portant l'extension TXT situés dans des répertoires imbriqués dans le répertoire dir, à l'exclusion du répertoire dir lui-même.

  - Le caractère `?` (point d'interrogation), qui remplace n'importe quel caractère unique, à l'exception des caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/???.txt` inclura les chemins d'accès à tous les fichiers situés dans le répertoire dir qui portent l'extension TXT et dont le nom se compose de trois caractères.

- **Exclusions par nom de menace** Saisissez le nom du type d'objet en fonction de la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, l'application exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.

Kaspersky Endpoint Security permet également d'exclure de l'analyse les fichiers de certains formats : archives, bases de données de messagerie, fichiers texte, fichiers journaux de bases de données.

Comment ajouter des exclusions de l'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Dans la liste des tâches, sélectionnez la tâche Analyse du conteneur de Kaspersky Endpoint Security et cliquez sur le nom de la tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zones d'exclusion**.

5. Ajoutez des exclusions par masque, si nécessaire :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions selon un masque**.

   b. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez les modèles des noms de fichiers que vous souhaitez exclure de l'analyse par Kaspersky Endpoint Security.

   c. Cliquez sur **Ajouter**.

   Les exclusions sont ajoutées à la liste.

6. Ajoutez des exclusions par nom de menace, si nécessaire :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions d'après le nom de la menace**.

   b. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez les modèles de noms de menace. L'application ne bloquera pas les menaces spécifiées.

   Par exemple, si vous utilisez un outil pour analyser votre réseau, ajoutez le nom complet de la menace correspondante à la liste des menaces à exclure de l'analyse.

   Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.

7. Si nécessaire, vous pouvez importer ou exporter des exclusions pour chacune des listes :

   - Pour exporter la liste des exclusions, cliquez sur le bouton **Exporter**.

     Kaspersky Endpoint Security enregistre le fichier export.json dans votre dossier des téléchargements par défaut.

   - Pour importer la liste des exclusions, procédez comme suit :

     a. Cliquez sur **Importer**.

     b. Sélectionnez le fichier JSON à partir duquel vous souhaitez importer des zones d'exclusion.

     c. Ouvrez le fichier.

     d. Sélectionnez la méthode d'importation : ajouter des exclusions à la liste existante ou remplacer la liste des exclusions.

     e. Enregistrez vos modifications.

     Les règles du fichier JSON s'affichent dans la liste.

8. Enregistrez vos modifications.

Comment ajouter des exclusions de l'analyse en ligne de commande

1. Ajoutez une zone d'exclusion à l'aide de la commande suivante :

```
kesl-control --set-settings <ID ou nom de la tâche> --add-exclusion <chemin d'accès>
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--add-exclusion <path>` ajoute le chemin d'accès au répertoire contenant les objets que vous souhaitez exclure de l'analyse.

Une nouvelle section `[ExcludedFromScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application exclura des analyses les objets du répertoire spécifié par le paramètre `Path`. Les autres paramètres de la zone d'exclusion prennent leurs valeurs par défaut.

Si les paramètres de la tâche ont déjà une section `[ExcludedFromScanScope.item_#]` avec la valeur spécifiée du paramètre `Path`, la section en double n'est pas ajoutée.

Si le paramètre `UseScanArea` a reçu la valeur `No`, il prend la valeur `Yes` après l'exécution de la commande et les objets situés dans ce répertoire sont exclus de l'analyse.

2. Vous pouvez également ajouter une zone d'exclusion à l'aide d'un fichier de configuration :

   a. Enregistrez les paramètres de la tâche dans un fichier de configuration en exécutant la commande suivante :

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Ouvrez le fichier de configuration afin de le modifier.

   c. Ajoutez une section `[ExcludedFromScanScope.item_#]` au fichier avec les paramètres suivants :

   - `AreaDesc` : spécifie la description de la zone d'exclusion, qui contient des informations supplémentaires sur la zone d'exclusion.
   - `UseScanArea` : activer l'exclusion de la zone spécifiée.
   - `Path` est le chemin d'accès au répertoire contenant les objets à exclure. Vous pouvez spécifier le chemin d'accès à un répertoire local ou exclure les répertoires distants montés sur l'appareil client. Les valeurs de paramètres possibles dépendent du type de tâche.
   - `AreaMask.item_#` : limitation de la zone d'exclusion. Vous pouvez spécifier un masque pour les noms des fichiers que vous souhaitez exclure de la portée de l'analyse. Par défaut, tous les objets de portée sont exclus.

     Exemple

     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   d. Vous pouvez spécifier plusieurs sections `[ExcludedFromScanScope.item_#]`.

   L'application traite les zones par ordre croissant d'index d'élément.

   e. Enregistrez les modifications dans le fichier de configuration.

f. Importez les paramètres du fichier de configuration dans la tâche à l'aide de la commande suivante :

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. Le cas échéant, vous pouvez supprimer une zone d'exclusion en exécutant la commande suivante :

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--del-exclusion <path>` supprime le chemin d'accès au répertoire contenant les objets à exclure de l'analyse.

Une section `[ExcludedFromScanScope.item_#]` qui contient le chemin indiqué sera supprimée depuis les paramètres de la tâche. L'application n'exclura pas les objets du répertoire spécifié de l'analyse.

Comment optimiser l'Analyse du conteneur

Configurez l'analyse des fichiers afin d'optimiser les performances de la tâche. Cela permet de réduire l'utilisation du processeur sur l'appareil protégé. Vous pouvez limiter l'analyse des archives, définir la taille maximale des objets pouvant être analysés et définir la durée maximale de l'analyse des objets. Kaspersky Endpoint Security permet également d'exclure de l'analyse les fichiers de certains formats : archives, bases de données de messagerie, fichiers texte et messages électroniques en texte brut.

Comment configurer l'analyse des fichiers dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Dans la liste des tâches, sélectionnez la tâche Analyse du conteneur de Kaspersky Endpoint Security et cliquez sur le nom de la tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sous **Paramètres d'analyse**, configurez l'analyse des fichiers :

   - **Analyser les archives**. Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). L'analyse est désactivée par défaut.
   - **Analyser les archives SFX**. Analyse des archives autoextractibles qui contiennent un module d'extraction exécutable. L'analyse est désactivée par défaut.
   - **Analyser les bases de messagerie**. Analyse des bases de données de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres clients de messagerie. L'analyse est désactivée par défaut.

- **Analyser les fichiers au format de messagerie**. Analyse des messages électroniques au format texte brut. L'analyse est désactivée par défaut.

- **Ignorer un fichier si son analyse prend plus de (secondes)**. Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre. Par défaut, l'application tente d'analyser un objet dans un délai d'une minute.

- **Ignorer un fichier si sa taille est supérieure à (Mo)**. Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.

- **Ignorer un fichier si sa taille est supérieure à (Mo)**. Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée.

5. Enregistrez vos modifications.

Comment configurer l'analyse des fichiers en ligne de commande

1. Exécutez la commande:

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

- `<object size (MB)>` est la taille maximale d'un objet à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse. Valeur par défaut : `0`.

- `<scan time (sec)>` est la durée maximale d'analyse d'un objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre. Valeur par défaut : `0`.

2. Vous pouvez également configurer les paramètres à l'aide d'un fichier de configuration :

   a. Exportez les paramètres de la tâche dans un fichier de configuration en exécutant la commande suivante :

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Ouvrez le fichier de configuration afin de le modifier.

   c. Ajoutez à ce fichier les paramètres suivants de la tâche *Analyse du conteneur*, qui s'appliquent aux objets à l'intérieur des conteneurs et des images : `ScanArchived`, `ScanSfxArchived`, `ScanMailBases`, `ScanPlainMail`, `SizeLimit`, `TimeLimit`, `QueueScanTasks`.

   d. Enregistrez les modifications dans le fichier de configuration.

e. Importez les paramètres du fichier de configuration dans la tâche à l'aide de la commande suivante :

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `--file <path>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de la tâche définies dans le fichier seront importées dans l'application.

Sélection de l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté

Lorsqu'un objet infecté est détecté dans un conteneur, Kaspersky Endpoint Security peut arrêter immédiatement le conteneur, ne rien faire ou arrêter le conteneur si la désinfection de l'objet ou l'élimination de la menace s'est avérée impossible. Vous pouvez sélectionner l'action que Kaspersky Endpoint Security exécute sur le conteneur lorsqu'un objet infecté est détecté dans le cadre de l'analyse en temps réel par le module *Surveillance des conteneurs* ou dans le cadre d'une tâche à la demande *Analyse du conteneur*.

Si un objet infecté est détecté dans l'image de conteneur, Kaspersky Endpoint Security peut supprimer l'image ou n'exécuter aucune action sur celle-ci. Vous pouvez sélectionner l'action que Kaspersky Endpoint Security exécute sur l'image de conteneur lorsqu'un objet infecté est détecté dans le cadre d'une tâche à la demande *Analyse du conteneur*.

Comment sélectionner une action de Surveillance des conteneurs lors de la détection d'une menace dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

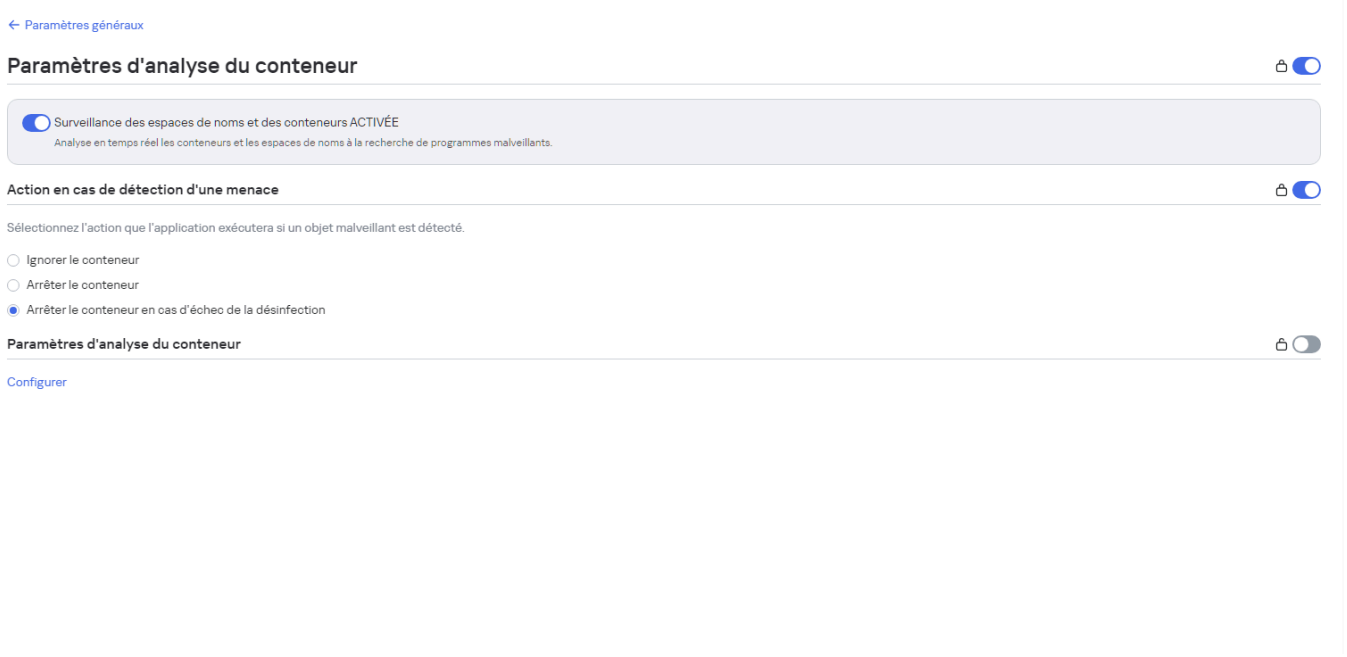
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres d'analyse du conteneur**.
5. Assurez-vous que le bouton bascule du module Surveillance des conteneurs se trouve en position **Surveillance des espaces de noms et des conteneurs ACTIVÉE**.

6. Dans la section **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera lorsqu'un objet infecté est détecté dans un conteneur :

   - **Ignorer le conteneur**. En cas de détection d'un objet infecté dans un conteneur, l'application n'exécute aucune action sur le conteneur.
   - **Arrêter le conteneur**. En cas de détection d'un objet infecté dans un conteneur, l'application arrête le conteneur.
   - **Arrêter le conteneur en cas d'échec de la désinfection** (par défaut). En cas de détection d'un objet infecté dans un conteneur, l'application tente de désinfecter l'objet infecté. Si un objet infecté n'a pas pu être désinfecté, l'application arrête le conteneur.

     En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action **Arrêter le conteneur**.

7. Enregistrez vos modifications.



Paramètres d'analyse de conteneur

Comment sélectionner une action de Surveillance des conteneurs lors de la détection d'une menace depuis la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

Ce paramètre ne peut être configuré que lors de l'utilisation de l'application sous une licence qui prend en charge cette fonction.

2. Pour vérifier les valeurs actuelles des paramètres de l'Analyse du conteneur, exécutez la commande suivante :

```
kesl-control --get-settings container-settings
```

Comment sélectionner une action d'Analyse du conteneur lors de la détection d'une menace dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Dans la liste des tâches, sélectionnez la tâche Analyse du conteneur de Kaspersky Endpoint Security et cliquez sur le nom de la tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sous **Paramètres d'analyse avancés → Paramètres d'analyse du conteneur → Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera lorsqu'un objet infecté est détecté dans un conteneur :

   - **Ignorer le conteneur**. En cas de détection d'un objet infecté dans un conteneur, l'application n'exécute aucune action sur le conteneur.
   - **Arrêter le conteneur**. En cas de détection d'un objet infecté dans un conteneur, l'application arrête le conteneur.
   - **Arrêter le conteneur en cas d'échec de la désinfection** (par défaut). En cas de détection d'un objet infecté dans un conteneur, l'application tente de désinfecter l'objet infecté. Si un objet infecté n'a pas pu être désinfecté, l'application arrête le conteneur.

     En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action **Arrêter le conteneur**.

5. Sous **Paramètres d'analyse avancés → Paramètres d'analyse d'image → Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera lorsqu'un objet infecté est détecté dans un conteneur :

   - **Ignorer l'image** (par défaut). En cas de détection d'un objet infecté dans l'image, l'application n'exécute aucune action sur l'image.
   - **Supprimer l'image** (déconseillé). En cas de détection d'un objet infecté dans l'image, l'application supprime l'image. Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.

6. Enregistrez vos modifications.

Comment sélectionner une action d'Analyse du conteneur lors de la détection d'une menace sur la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
ImageAction=<Skip|Delete>
```

Où `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

> En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action `StopContainer`.

2. Vous pouvez également configurer l'action à l'aide d'un fichier de configuration :

   a. Exportez les paramètres de la tâche dans un fichier de configuration en exécutant la commande suivante :

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Ouvrez le fichier de configuration afin de le modifier.

   c. Ajoutez les paramètres suivants de la tâche *Analyse du conteneur* au fichier :

   - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – action à effectuer sur un conteneur lorsqu'un objet infecté est détecté. Valeur par défaut : `StopContainerIfFailed`.
   - `ImageAction=<Skip|Delete>` – action à effectuer sur une image de conteneur lorsqu'un objet infecté est détecté. Valeur par défaut : `Skip`.

   d. Enregistrez les modifications dans le fichier de configuration.

   e. Importez les paramètres du fichier de configuration dans la tâche à l'aide de la commande suivante :

   ```
   kesl-control --set-settings <task ID|name> --file <path> [--json]
   ```

   Où :

   - `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
   - `--file <path>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.
   - `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de la tâche définies dans le fichier seront importées dans l'application.

Exécution d'une analyse personnalisée des conteneurs et des images

Pour lancer la tâche Analyse personnalisée du conteneur depuis la ligne de commande, exécutez la commande suivante :

```
kesl-control --scan-container <id|name[:tag]>
```

où `<id|name[:tag]>` est le nom ou l'identifiant du conteneur ou de l'image. Vous pouvez utiliser des masques pour analyser plusieurs objets.

S'il existe plusieurs entités portant le même nom, l'application les analyse toutes.

À la suite de l'exécution de la commande, une tâche temporaire d'analyse du conteneur et des images est créée, qui est automatiquement supprimée une fois terminée. Parallèlement, les résultats de l'analyse sont affichés dans la console.

Exemple d'analyse d'un conteneur effectuée sur un conteneur nommé my_container

```
kesl-control --scan-container my_container
```

Exemple d'analyse d'une image effectuée sur une image nommée my_image (tous les tags)

```
kesl-control --scan-container my_image*
```

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Analyse des disques amovibles

Kaspersky Endpoint Security analyse tous les fichiers que vous exécutez ou copiez, même si le fichier se trouve sur un disque amovible. L'application analyse les fichiers sur les CD, DVD, disques Blu-ray, lecteurs flash (y compris les modems USB), disques durs externes et disquettes. Par défaut, l'analyse des disques amovibles est désactivée.

Fonctionnement de l'analyse des disques amovibles

Quand un disque amovible est connecté, l'application crée et lance automatiquement les tâches d'analyse suivantes avec les paramètres par défaut : *Analyse des zones critiques* pour l'analyse rapide et *Analyse des logiciels malveillants* pour l'analyse complète. Ces tâches ne peuvent pas être arrêtées. Lorsqu'une menace est détectée sur le disque amovible, Kaspersky Endpoint Security tente de désinfecter l'objet infecté. Si la désinfection s'avère impossible, l'application supprime l'objet infecté. Une fois l'analyse terminée, l'application supprime automatiquement ces tâches.

Types d'analyse

- **Analyse rapide**. Kaspersky Endpoint Security analyse uniquement les fichiers avec les extensions indiquées et ne décompresse pas les objets composés. L'application exécute une analyse rapide avec les paramètres par défaut de la tâche *Analyse des zones critiques*.
- **Analyse complète**. Kaspersky Endpoint Security analyse tous les fichiers sur les disques amovibles. L'application exécute une analyse complète avec les paramètres par défaut de la tâche *Analyse des logiciels malveillants*.

Comment sélectionner un type d'analyse des disques amovibles dans la Web Console

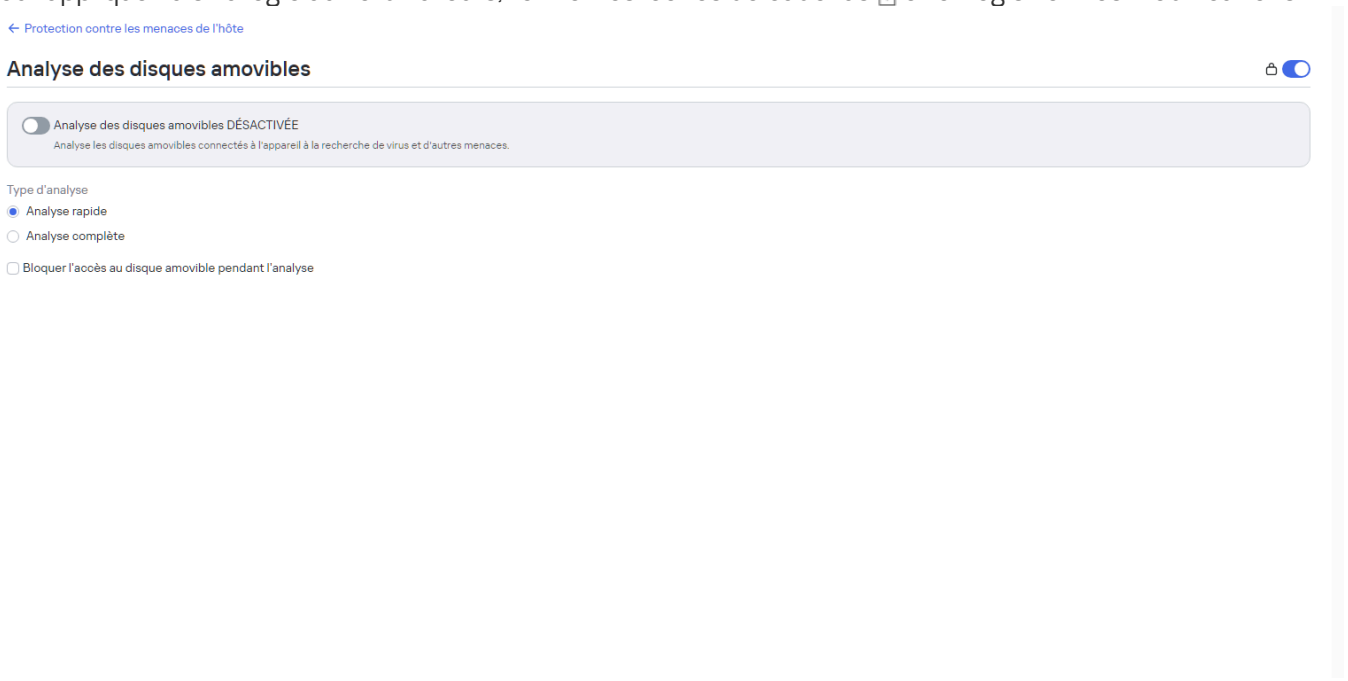
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse des disques amovibles**.
5. Assurez-vous que le commutateur du module est en position **Analyse des disques amovibles ACTIVÉE**.
6. Sous **Type d'analyse**, sélectionnez le type d'analyse des disques amovibles : **Analyse rapide** ou **Analyse complète**.
7. Le cas échéant, cochez la case **Bloquer l'accès aux fichiers pendant l'analyse**.

   Le blocage de l'accès aux fichiers empêche l'utilisateur d'exécuter des applications malveillantes pendant l'analyse.

Lors de l'analyse des secteurs d'amorçage, l'application ne bloque aucun fichier.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Analyse des disques amovibles

Comment sélectionner un type d'analyse des disques amovibles sur la ligne de commande

1. Sélectionnez le type d'analyse à effectuer lors de la connexion de disques amovibles :

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. Sélectionnez le type d'analyse à effectuer lors de l'insertion de lecteurs CD/DVD ou de disques Blu-ray :

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 16
```

Symboles

Options de la commande

Paramètre	Description
`ScanRemovableDrives`	Type d'analyse lors de la connexion de disques amovibles : • `DetailedScan`. Analyse complète. • `QuickScan`. Analyse rapide. • `NoScan` (par défaut). L'application n'effectue pas d'analyse.
`ScanOpticalDrives`	Type d'analyse à effectuer lors de l'insertion de lecteurs CD/DVD ou de disques Blu-ray : • `DetailedScan`. Analyse complète. • `QuickScan`. Analyse rapide. • `NoScan` (par défaut). L'application n'effectue pas d'analyse.

Paramètre	Description
`BlockDuringScan`	Bloquer l'accès aux fichiers du disque connecté pendant l'analyse. Par défaut, l'application ne bloque pas l'accès aux fichiers. Le blocage de l'accès aux fichiers empêche l'utilisateur d'exécuter des applications malveillantes pendant l'analyse. Lors de l'analyse des secteurs d'amorçage, l'application ne bloque aucun fichier.

Détection comportementale

Le module Détection comportementale permet de surveiller l'activité (ouverture de fichiers, établissement de connexions, etc.) des applications qui peuvent compromettre l'ordinateur ou les données de l'utilisateur. Le module surveille le comportement des applications afin de détecter des schémas dangereux. Si l'activité d'une application correspond à l'un de ces schémas, Kaspersky Endpoint Security exécute l'action de réponse sélectionnée. Cette fonctionnalité de Kaspersky Endpoint Security assure une protection proactive de l'ordinateur.

Pour optimiser les performances du module Détection comportementale, nous vous recommandons d'activer le module Protection contre les menaces Internet.

Fonctionnement de la Détection comportementale

1. **L'application surveille les événements dans le système d'exploitation**

   L'application reçoit un flux de télémétrie composé d'événements : création et arrêt de processus, fichiers ouverts, connexions établies, etc. L'application enrichit également les événements avec les métadonnées pertinentes (nom du processus, PID, adresse IP, etc.).

2. **L'application compare le flux de télémétrie avec des schémas de comportement dangereux**

   Si les actions d'une application tierce correspondent à un schéma de comportement dangereux, Kaspersky Endpoint Security exécute une action de réponse à la menace (par exemple, il peut arrêter l'application tierce).

3. **L'application envoie les données de télémétrie à KSN**

   L'application filtre les événements et les envoie à KSN pour une analyse approfondie.

Configuration de la Détection comportementale

1. **Dans les paramètres de Détection comportementale, sélectionnez l'action Informer**

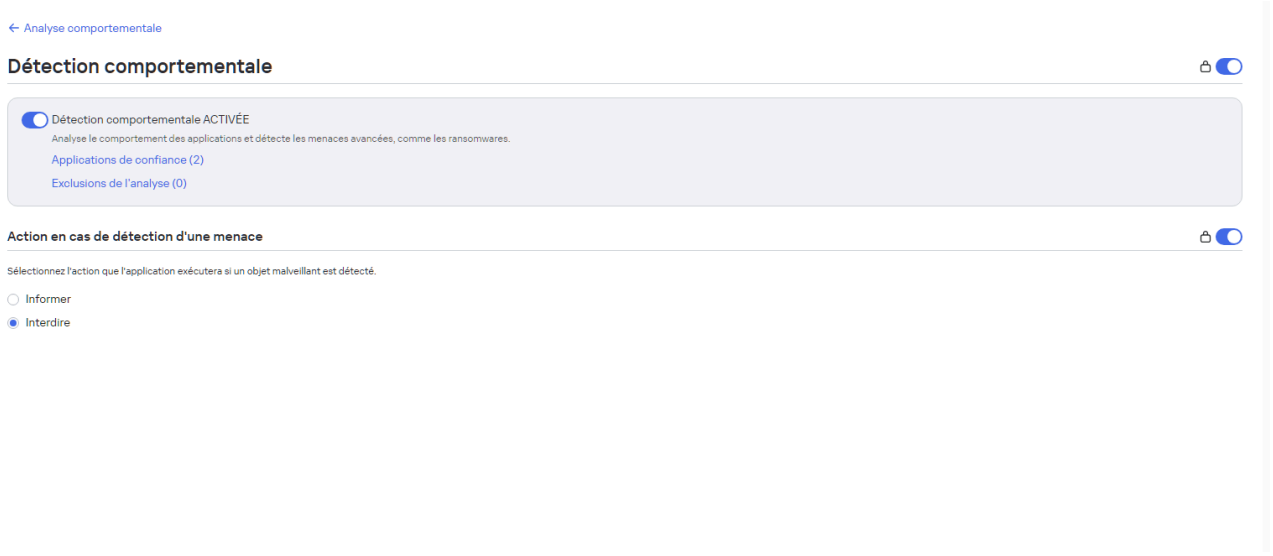
   Le module Détection comportementale est activé par défaut. Dans les paramètres de Détection comportementale, nous vous recommandons de sélectionner **Informer** comme action lors de la détection d'une menace et de vérifier si les applications installées fonctionnent normalement. Kaspersky Endpoint Security autorise toutes les activités des applications et tient un journal du fonctionnement du module.

Sélection d'une action en cas de détection d'une activité d'application malveillante dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte → Analyse comportementale → Détection comportementale**.
5. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

   - **Informer**. Si une activité malveillante est détectée, Kaspersky Endpoint Security n'arrête pas cette application, mais enregistre uniquement un événement concernant la détection d'une activité malveillante dans le journal des événements.
   - **Interdire**. Si une activité malveillante est détectée, Kaspersky Endpoint Security arrête le processus de l'application qui exécute l'activité malveillante et consigne les informations relatives à l'activité malveillante détectée.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Détection comportementale

Sélection d'une action en cas de détection d'une activité d'application malveillante sur la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 20
```

Symboles

Options de la commande

Paramètre	Description
`TaskMode`	Action en cas de détection d'une activité d'application malveillante : • `Block` (par défaut). Si une activité malveillante est détectée, Kaspersky Endpoint Security arrête le processus de l'application qui exécute l'activité malveillante et consigne les informations relatives à l'activité malveillante détectée. • `Notify`. Si une activité malveillante est détectée, Kaspersky Endpoint Security n'arrête pas cette application, mais enregistre uniquement un événement concernant la détection d'une activité malveillante dans le journal des événements.

2. **Collecter les statistiques de la Détection comportementale**

   Vous pouvez obtenir les statistiques de la Détection comportementale à l'aide de rapports.

3. **Optimiser les performances de l'application**

   Après avoir analysé les informations recueillies, optimisez les performances de l'application et ajoutez des exclusions.

4. **Dans les paramètres de Détection comportementale, sélectionnez l'action Bloquer**

   Activez le blocage de l'activité malveillante des applications. Ensuite, Kaspersky Endpoint Security arrêtera les processus des applications qui exécutent une activité malveillante.

Considérations particulières et limitations

- Pour assurer le bon fonctionnement du module Détection comportementale lorsque Kaspersky Endpoint Security est intégré aux solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform, assurez-vous que auditd est défini sur le mode sans blocage de la configuration `enabled 1` dans les fichiers de configuration.

Protection contre les Exploits

La Protection contre les Exploits surveille le code qui exploite les vulnérabilités de votre appareil afin d'obtenir des privilèges d'administrateur ou d'effectuer des actions malveillantes.

Pour que le module Protection contre les Exploits fonctionne, les modules suivants doivent être activés :

- Détection comportementale
- Module de noyau mis à jour

> Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Fonctionnement de la Protection contre les Exploits

1. **L'application surveille les événements dans le système d'exploitation**

   L'application reçoit un flux de télémétrie composé d'événements : création et arrêt de processus, fichiers ouverts, connexions établies, etc. L'application enrichit également les événements avec les métadonnées pertinentes (nom du processus, PID, adresse IP, etc.).

2 L'application compare le flux de télémétrie avec des schémas de comportement dangereux

Si les actions d'une application tierce correspondent à un schéma de comportement dangereux, Kaspersky Endpoint Security exécute une action de réponse à la menace (par exemple, il peut arrêter l'application tierce).

Configuration de la Protection contre les Exploits

1 Dans les paramètres de la Protection contre les Exploits, sélectionnez l'action Informer

Par défaut, le module Protection contre les Exploits est désactivé. Dans les paramètres de la Protection contre les Exploits, sélectionnez **Informer** comme action lors de la détection d'une menace et vérifiez si les applications installées peuvent fonctionner normalement. Kaspersky Endpoint Security autorise toutes les activités des applications et consigne les informations relatives aux menaces détectées.

Comment sélectionner l'action lors de la détection d'un exploit dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte → Analyse comportementale → Protection contre les Exploits**.
5. Utilisez le commutateur **Protection contre les Exploits** pour activer ou désactiver le module.
6. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

   - **Interdire**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après la détection d'un exploit, bloque l'opération de ce code d'exploitation et crée dans le journal une entrée qui reprend des informations relatives à ce code d'exploitation.
   - **Informer**. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert un exploit, crée une entrée dans le journal qui reprend les informations relatives à l'exploit et ajoute les informations relatives à l'exploit dans la liste des menaces actives.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner l'action lors de la détection d'une menace depuis la ligne de commande

1. Pour activer la Protection contre les Exploits, exécutez la commande suivante :

   ```
   kesl-control --set-settings 20 UseAEP=Yes
   ```
2. Sélectionnez une action lors de la détection d'un exploit :

   ```
   kesl-control --set-settings 20 AEPMode=<Block|Notify>
   ```

3. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 20
```

Symboles

Options de la commande

Paramètre	Description
`UseAEP`	Activation du module : • `Yes` active la Protection contre les Exploits. • `No` (valeur par défaut) : désactiver la Protection contre les Exploits.
`AEPMode`	Action lors de la détection d'un exploit : • `Block` (par défaut). Kaspersky Endpoint Security bloque les opérations de cet exploit et crée une entrée dans le journal avec des informations relatives à cet exploit. • `Notify`. Lorsque Kaspersky Endpoint Security détecte un exploit, l'application crée une entrée dans le journal contenant des informations relatives à l'exploit et ajoute les informations relatives à cet exploit à la liste des menaces actives.

2. **Collecter les statistiques de la Protection contre les Exploits**

   Vous pouvez obtenir les statistiques de la Protection contre les Exploits à l'aide des rapports.

3. **Optimiser les performances de l'application**

   Après avoir analysé les informations recueillies, optimisez les performances de l'application :

   - Ajouter des exclusions globales
   - Ajouter des exclusions

4. **Dans les paramètres de la Protection contre les Exploits, sélectionnez l'action Bloquer**

   Activer le blocage de l'activité malveillante des applications dans le système d'exploitation.

Protection contre le chiffrement

Le module Protection contre le chiffrement assure la protection contre le chiffrement à distance en analysant l'activité des appareils distants dans les répertoires réseau partagés de l'ordinateur. La Protection contre le chiffrement analyse les fichiers transmis à l'ordinateur protégé via les protocoles NFS et SMB.

Si l'activité correspond à un modèle de comportement caractéristique du chiffrement externe, Kaspersky Endpoint Security bloque cette activité ou vous en informe.

Fonctionnement de la Protection contre le chiffrement

1. **L'application intercepte les requêtes NFS et SMB**

   L'application reçoit un flux de télémétrie sur la création et la modification des fichiers transmis via les protocoles NFS et SMB.

2. **L'application compare le flux de télémétrie avec les bases de signatures.**

   Si les actions de l'application tierce correspondent à celles d'un ransomware, Kaspersky Endpoint Security exécute l'action sélectionnée lors de la détection d'une menace (par exemple, le blocage de la connexion à l'ordinateur distant).

Configuration de la Protection contre le chiffrement

1. **Configurer la zone de protection**

   Par défaut, l'application analyse tous les répertoires partagés. Si vous devez analyser uniquement un répertoire spécifique (par exemple, le répertoire dans lequel les fichiers sont automatiquement téléchargés depuis une source externe), vous pouvez définir uniquement ce répertoire comme zone de protection. Dans les autres cas, nous vous recommandons de conserver la zone de protection par défaut et d'utiliser des exclusions pour affiner cette zone.

2. **Dans les paramètres de la Protection contre le chiffrement, sélectionnez l'action Informer**

   Par défaut, la Protection contre le chiffrement est désactivée. Nous vous recommandons d'activer la Protection contre le chiffrement et, comme action lors de la détection d'une menace, de sélectionner **Informer**, puis de vérifier l'accès à toutes les ressources de l'entreprise. Kaspersky Endpoint Security autorise l'accès à toutes les ressources des répertoires partagés et consigne les informations relatives aux menaces détectées.

3. **Collecter les statistiques de la Protection contre le chiffrement**

   Vous pouvez obtenir les statistiques de la Protection contre le chiffrement à l'aide des rapports.

4. **Optimiser les performances de l'application**

   Après avoir analysé les informations recueillies, optimisez les performances de l'application :

   - Ajouter des exclusions globales.
   - Ajouter des exclusions.

5. **Dans les paramètres de la Protection contre le chiffrement, sélectionnez l'action Bloquer la connexion**

   Activez le blocage du trafic réseau provenant d'un appareil distant à l'origine d'une attaque.

Considérations particulières et limitations

- Le module Protection contre le chiffrement fonctionne correctement avec les protocoles SMB1, SMB2, SMB3, NFS3, TCP/UDP et IP. Les protocoles NFS2 et NFS4 ne sont pas pris en charge. Il est conseillé de configurer le serveur de telle sorte que les protocoles NFS2 et NFS4 ne puissent pas être utilisés pour monter des ressources.
- Pour que le module Protection contre le chiffrement fonctionne correctement, au moins l'un des services (Samba ou NFS) doit être installé dans le système d'exploitation. Pour le service NFS, le paquet rpcbind doit être installé.
- L'application Kaspersky Endpoint Security ne bloque pas l'accès aux ressources de fichiers réseau tant que l'activité d'un appareil distant n'a pas été considérée comme malveillante. Autrement dit, au moins un fichier doit être chiffré avant que l'application ne détecte une activité malveillante.

Comment sélectionner une action lors de la détection d'un chiffrement malveillant

Si un chiffrement malveillant est détecté, l'application peut bloquer le trafic réseau de l'appareil distant attaquant ou simplement signaler la détection du chiffrement malveillant.

Pour bloquer le trafic réseau, Kaspersky Endpoint Security crée une règle de pare-feu dynamique. Le pare-feu bloque temporairement le trafic réseau de l'appareil attaquant. L'application ajoute également l'appareil attaquant à la liste des appareils bloqués. L'accès aux répertoires réseau partagés est refusé aux appareils bloqués.

Pour informer l'administrateur de la détection d'un chiffrement malveillant, l'application génère un événement *Chiffrement détecté*.

Par défaut, l'application bloque le trafic réseau d'un appareil attaquant pendant 60 minutes. Une fois le délai de blocage expiré, l'application supprime l'appareil compromis de la liste des appareils bloqués et l'accès de l'appareil aux ressources de fichiers réseau est automatiquement restauré.

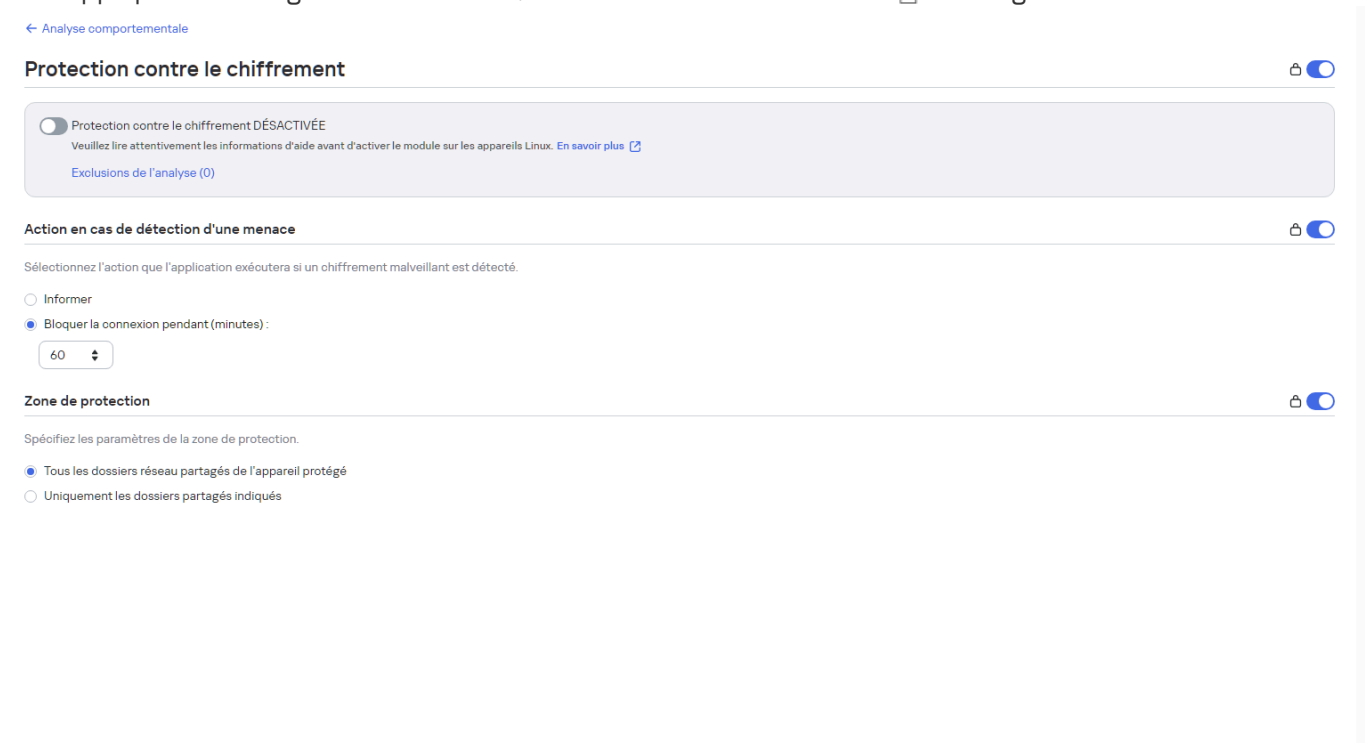
Vous pouvez consulter la liste des appareils bloqués et débloquer manuellement ces appareils localement sur l'ordinateur de l'utilisateur. Kaspersky Security Center ne fournit pas d'outils de surveillance et de gestion des appareils bloqués, à l'exception de l'événement *Chiffrement détecté*.

Comment configurer les actions en cas de détection d'un chiffrement malveillant dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.
5. Assurez-vous que le commutateur du module est en position **Protection contre le chiffrement ACTIVÉE**.
6. Sous **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera lorsqu'une menace est détectée : **Informer** ou **Bloquer la connexion pendant (minutes)**.
7. Si **Bloquer la connexion pendant (minutes)** est sélectionné, définissez la durée de blocage de l'appareil attaquant en minutes. Par défaut, l'appareil est bloqué pendant 60 minutes.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection contre le chiffrement

Comment configurer les actions en cas de détection d'un chiffrement malveillant en ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. Sélectionnez la durée de blocage pour l'action `Block`.

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 13
```

Symboles

Options de la commande

Paramètre	Description
`ActionOnDetect`	Action en cas de détection d'un chiffrement externe : • `Block` (par défaut) bloque le trafic réseau de l'appareil attaquant et crée un événement *Chiffrement détecté*. • `Notify` crée un événement *Chiffrement détecté* sans bloquer le trafic réseau.
`BlockTime`	Durée de blocage des appareils attaquants en minutes.

Comment créer une zone de protection

Une *zone de protection* est une liste de chemins d'accès aux répertoires réseau partagés dans lesquels Kaspersky Endpoint Security surveille l'activité des fichiers. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. Par défaut, l'application identifie automatiquement les répertoires réseau partagés et surveille l'activité des fichiers dans ces répertoires.

Si nécessaire, vous pouvez limiter la surveillance de l'activité des fichiers à la recherche d'un chiffrement malveillant à un sous-ensemble de répertoires. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

L'exclusion d'un répertoire de la zone de protection peut réduire le nombre de faux positifs si votre entreprise utilise le chiffrement des données lors de l'échange de fichiers via des répertoires réseau partagés. Par exemple, la Protection contre le chiffrement peut générer des faux positifs lorsque l'utilisateur travaille avec des fichiers portant l'extension ENC dans un dossier partagé. Une telle activité correspond à un modèle comportemental typique de chiffrement externe. Si vous avez des fichiers chiffrés dans un répertoire réseau partagé pour protéger les données, ajoutez ce répertoire aux exclusions.

Comment créer une zone de protection dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.
5. Assurez-vous que le commutateur du module est en position **Protection contre le chiffrement ACTIVÉE**.
6. Sous **Zone de protection**, sélectionnez **Uniquement les dossiers partagés indiqués**.
7. Dans la liste des répertoires, cliquez sur **Ajouter**.
8. Une fenêtre s'ouvre ; dans celle-ci, sélectionnez le type de système de fichiers :

   - **Local**. Répertoires sur le disque dur accessibles sans connexion réseau.
   - **Partagé**. Répertoires de l'ordinateur accessibles via les protocoles Samba (SMB) ou NFS.
   - **Tous les éléments partagés**. Tous les répertoires de l'ordinateur accessibles via les protocoles Samba et NFS.
9. Pour un système de fichiers local, indiquez le chemin d'accès à un répertoire (par exemple, `/path/to/folder`).
10. Spécifiez les masques des extensions d'objet (par exemple, `*.txt`). Séparez les masques par des virgules.
11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment créer une zone de protection via la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 13
```

Symboles

Options de la commande

Paramètre	Description
`ScanScope.item_#.UseScanArea=Yes`	Activation de la zone de protection numéro `#`. Vous pouvez exclure temporairement une zone de protection au lieu de la supprimer. Pour ce faire, définissez `ScanScope.item_#.UseScanArea=No`.
`ScanScope.item_#.AreaDesc`	Description de la zone de protection ; contient des informations complémentaires sur la zone de protection `#`.

`ScanScope.item_#.AreaMask.item_#`	Restriction de la zone de protection. Dans la zone de protection, l'application protège uniquement les objets renseignés à l'aide de masques au format shell.
	`Exemple`
	`ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`

`ScanScope.item_#.Path`	Chemin d'accès au répertoire contenant les objets protégés. Valeurs possibles : • `AllShared` (par défaut). Tous les répertoires de l'ordinateur accessibles via les protocoles Samba et NFS. • `Shared:SMB`. Répertoires accessibles via le protocole Samba (SMB). • `Shared:NFS`. Répertoires accessibles via le protocole NFS. • `<path to local directory>`. Répertoires sur le disque dur accessibles sans connexion réseau. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

`Exemple d'une zone de protection qui inclut uniquement le répertoire /home`

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Protection BadUSB

Les attaquants peuvent exploiter les vulnérabilités du micrologiciel d'un appareil USB (par exemple, une clé USB) et reprogrammer le appareil afin que le système d'exploitation le reconnaisse comme un clavier lorsqu'il est connecté. Par conséquent, un appareil USB infecté peut exécuter des commandes sous votre compte utilisateur, par exemple pour télécharger une application malveillante.

Le module Protection BadUSB permet d'empêcher la connexion d'un appareil USB infecté.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Fonctionnement de la Protection BadUSB

1. **L'application vous invite à autoriser l'appareil USB**

   Lorsqu'un appareil USB est connecté à l'appareil, l'application invite l'utilisateur à saisir un code numérique généré par l'application. Cette procédure est appelée *autorisation*.

2. **L'utilisateur saisit le code d'autorisation**

   L'utilisateur peut saisir le code à l'aide de l'appareil USB connecté lui-même (clavier ou lecteur de codes-barres) ou d'un clavier visuel, le cas échéant. Il est impossible de saisir le code à l'aide d'un appareil USB déjà connecté.

3. **L'application autorise les appareils USB autorisés et bloque les appareils USB non autorisés**

   Si le code numérique est saisi correctement, l'application enregistre les paramètres d'identification, c'est-à-dire le VID/PID de l'appareil USB et le numéro du port auquel il est connecté, dans la liste des appareils USB autorisés. Cet appareil USB n'aura pas besoin d'être autorisé à nouveau s'il est reconnecté ou si le système d'exploitation est redémarré.

   Si le code numérique est saisi incorrectement, l'application en génère un nouveau. Vous pouvez configurer le nombre maximal de tentatives de saisie du code numérique. Si le code numérique est saisi incorrectement à plusieurs reprises, l'application bloque les entrées provenant de cet appareil USB pendant un certain temps. Une fois la durée de blocage du appareil USB écoulée, vous pouvez effectuer d'autres tentatives pour autoriser l'appareil USB. Vous pouvez configurer le délai à l'issue duquel vous pouvez poursuivre les tentatives de saisie du code d'autorisation.

Lorsqu'un appareil USB autorisé est connecté à un autre port USB, l'application exige qu'il soit à nouveau autorisé.

Configuration de la Protection BadUSB

1. **Activer la protection BadUSB**

   Par défaut, le module Protection BadUSB est désactivé. Identifiez les appareils auxquels des personnes non fiables peuvent accéder physiquement et qui doivent être protégés contre les attaquants externes, puis activez le module Protection BadUSB sur ces appareils. Après l'activation de la Protection BadUSB, l'application exigera l'autorisation des appareils USB connectés, et les utilisateurs ne pourront pas utiliser les appareils USB non autorisés tant que ceux-ci n'auront pas été autorisés. Toutefois, les appareils USB connectés avant l'activation de la Protection BadUSB sont considérés comme autorisés par défaut et ne nécessitent pas d'autorisation.

   Ne connectez aucun appareil USB non fiable à l'appareil tant que vous n'avez pas activé et configuré la Protection BadUSB.

2. **Configurer la Protection BadUSB**

   En fonction du type d'appareils USB connectés (claviers ou lecteurs de codes-barres), configurez le mode d'affichage du code d'autorisation : sous forme de code-barres ou de code numérique (paramètre par défaut).

   Si nécessaire, configurez l'autorisation des appareils USB :

   - Nombre maximal de tentatives de saisie du code d'autorisation
   - Durée de blocage de l'appareil USB lorsque le nombre maximal de tentatives est atteint.

Configuration de l'autorisation des appareils USB

Lorsqu'un appareil USB que le système d'exploitation identifie comme appareil d'entrée est connecté à l'appareil administré, l'application propose d'autoriser l'appareil USB à l'aide d'un code numérique ou d'un code-barres. Si le code d'autorisation n'est pas saisi correctement, l'application génère un nouveau code. Si le code d'autorisation est saisi incorrectement à plusieurs reprises ou si la fenêtre d'autorisation est fermée, l'application bloque la saisie provenant de cet appareil USB. Lorsque la durée de blocage de l'appareil USB arrive à échéance ou que le système d'exploitation redémarre, l'application invite l'utilisateur à procéder de nouveau à l'autorisation.

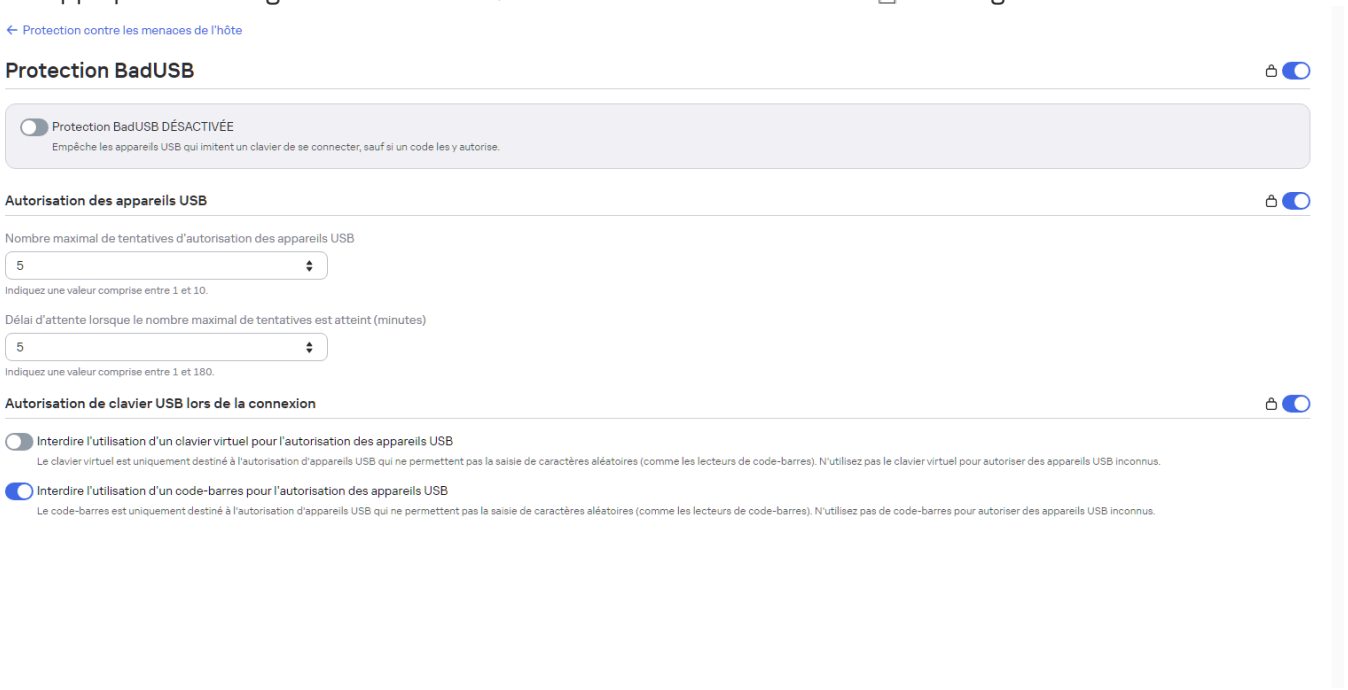
Kaspersky Endpoint Security permet de configurer l'autorisation des appareils USB

- Nombre maximal de tentatives d'autorisation.
- Durée de blocage de l'appareil USB lorsque le nombre maximal de tentatives est atteint.

Configuration de l'autorisation des appareils USB dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte → Protection BadUSB**.
5. Assurez-vous que le commutateur du module est en position **Protection BadUSB ACTIVÉE**.
6. Sous **Autorisation des appareils USB**, configurez les paramètres d'autorisation :
   - **Nombre maximal de tentatives d'autorisation des appareils USB**. Bloque automatiquement un appareil USB si le code d'autorisation est saisi incorrectement un nombre de fois spécifié. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affichera la durée de verrouillage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.
   - **Délai d'attente lorsque le nombre maximal de tentatives est atteint (minutes)**. La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs autorisées vont de 1 à 180 minutes.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection BadUSB

Configuration de l'autorisation des appareils USB via la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 37
```

Symboles

Options de la commande

Paramètre	Description
`MaxAuthAttempts`	Bloque automatiquement un appareil USB si le code d'autorisation est saisi incorrectement un nombre de fois spécifié. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affichera la durée de verrouillage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation. Valeur par défaut : 5.
`TimeoutAfterAttempts`	La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs autorisées vont de 1 à 180 minutes. Valeur par défaut : 5 minutes.

Autorisation de la connexion d'appareils USB à l'aide du clavier visuel

La possibilité d'utiliser le clavier virtuel existe uniquement pour l'autorisation des appareils USB qui ne prennent pas en charge la saisie de caractères (par exemple, un lecteur de code-barres). Il est déconseillé d'utiliser le clavier virtuel pour autoriser des appareils USB que vous ne connaissez pas. Par défaut, l'utilisation du clavier virtuel est autorisée.

Nous recommandons d'utiliser le clavier virtuel uniquement pour autoriser les appareils USB connus de l'utilisateur.

Comment activer l'autorisation des appareils USB à l'aide du clavier virtuel dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection BadUSB**.
5. Assurez-vous que le commutateur du module est en position **Protection BadUSB ACTIVÉE**.
6. Assurez-vous que l'interrupteur **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB** est désactivé. Le bouton bascule est désactivé par défaut.
7. Pour appliquer la stratégie aux appareils, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'autorisation des appareils USB à l'aide du clavier virtuel à partir de la ligne de commande

Exécutez la commande :

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

Autorisation de la connexion d'appareils USB à l'aide du lecteur de codes-barres

Lors de la connexion d'un lecteur de codes-barres à l'appareil, le module Protection BadUSB identifie ce lecteur comme un appareil d'entrée et vous invite à procéder à une autorisation. Pour autoriser le lecteur de code-barres, il faut scanner un code-barres affiché à l'écran. L'application génère un code-barres au format Code39. La plupart des lecteurs de codes-barres et des lecteurs de codes QR prennent en charge ce format.

L'application prend également en charge une autre méthode d'autorisation des lecteurs de codes-barres. Si vous utilisez des appareils à écran tactile, vous pouvez utiliser le clavier virtuel pour saisir un code. Pour ce faire, vous devez autoriser le clavier virtuel. Cette méthode est pratique, par exemple, dans le cas de lecteurs de code-barres fixes intégrés dans les caisses enregistreuses. Les autres modes d'autorisation de lecteurs de code-barres sont interdits. Par défaut, l'application n'utilise pas de code-barres pour l'autorisation des appareils USB.

Comment activer l'autorisation des appareils USB à l'aide du lecteur de codes-barres dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection BadUSB**.
5. Assurez-vous que le commutateur du module est en position **Protection BadUSB ACTIVÉE**.
6. Désactivez le commutateur **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB**.
7. Pour appliquer la stratégie aux appareils, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'autorisation des appareils USB à l'aide du lecteur de codes-barres sur la ligne de commande

Exécutez la commande :

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

Protection des connexions réseau et des moyens de communications

Protection contre les menaces par emails

La Protection contre les menaces par emails analyse les pièces jointes des messages entrants et sortants à la recherche de virus et d'autres pièces jointes malveillantes. Ce module protège l'appareil grâce aux bases antivirus, au service cloud Kaspersky Security Network et à l'analyse heuristique.

La Protection contre les menaces par emails peut analyser les messages entrants et sortants. L'application prend en charge les protocoles POP3, SMTP et IMAP dans les clients de messagerie suivants : l'application prend également en charge les versions étendues des protocoles : POP3S, SMTPS et IMAPS.

Le module Protection contre les menaces par emails n'analyse pas les messages si le client de messagerie est ouvert dans un navigateur.

> Pour que la Protection contre les menaces par emails fonctionne, les ports réseau 25, 110, 143, 465, 587, 993 et 995 doivent être surveillés dans les paramètres réseau. Ces ports sont ajoutés par défaut à la liste des ports surveillés. Leur suppression de la liste peut perturber le fonctionnement du module.

Par défaut, le module Protection contre les menaces par emails est activé.

Fonctionnement de la Protection contre les menaces par emails

Lors de l'installation de Kaspersky Endpoint Security, l'application ajoute un certificat auto-signé, *Certificat racine personnel de Kaspersky Anti-Virus*. L'application place ce certificat dans le magasin local des certificats de confiance (`/etc/ssl/certs`). À chaque démarrage, l'application vérifie la présence du certificat. Si le certificat a été supprimé, l'application le restaure automatiquement.

1. **L'application intercepte le trafic de messagerie**

   Kaspersky Endpoint Security vérifie la connexion via les protocoles POP3, SMTP et IMAP.

2. **L'application analyse les messages entrants et sortants**

   La Protection contre les menaces par emails analyse le trafic à l'aide des technologies suivantes :

   - Bases antivirus.
   - Services cloud de Kaspersky Security Network.
   - La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

3. **L'application termine l'analyse**

   Si un message entrant contient une menace dans une pièce jointe ou dans le corps du message, Kaspersky Endpoint Security exécute l'action lors de la détection d'une menace. Si une menace est détectée dans un message sortant, la Protection contre les menaces par emails bloque l'envoi de ce message.

Configuration de la Protection contre les menaces par emails

1. **Définir un groupe pour le déploiement de test du module**

   Isolez un petit groupe d'appareils sur lesquels vous testerez la configuration du module Protection contre les menaces par emails. Cela vous permettra de vérifier que le module est correctement configuré et d'assurer le fonctionnement stable du client de messagerie, en évitant les défaillances éventuelles.

2. **Configurer le filtre des pièces jointes**

   Par défaut, le filtre de la Protection contre les menaces par emails configuré par Kaspersky fournit le niveau de protection recommandé. Si vous avez des exigences particulières en matière de sécurité de la messagerie, vous pouvez modifier les paramètres du filtre des pièces jointes.

3. **Configurer l'analyse des messages**

   Si nécessaire, configurez l'analyse des messages email conformément aux paramètres de votre serveur de messagerie. Par exemple, vous pouvez limiter la taille des archives analysées afin de réduire la charge sur le serveur de messagerie.

4. **Vérifier que la Protection contre les menaces par emails fonctionne correctement**

   Générez un message de test avec une pièce jointe malveillante. Envoyez le message au groupe d'appareils que vous avez sélectionné et vérifiez que le contenu malveillant du message a été traité conformément aux paramètres du module.

   Vous pouvez également vérifier que l'application a généré l'événement *Une menace a été détectée* correspondant en exécutant la commande suivante :

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **Appliquer les paramètres de la Protection contre les menaces par emails à tous les appareils de l'organisation**

Considérations particulières et limitations

- Si le client de messagerie des appareils protégés n'utilise pas de magasin local de certificats de confiance, ajoutez manuellement le certificat *Certificat racine personnel de Kaspersky Anti-Virus* au magasin de certificats de confiance du client de messagerie. Pour en savoir plus sur l'ajout d'un certificat, consultez la documentation officielle de votre client de messagerie.
- La Protection contre les menaces par emails ne tente pas de désinfecter les pièces jointes malveillantes dans les messages sortants. Les messages sortants contenant des pièces jointes malveillantes sont soit complètement bloqués, soit autorisés.

Que faire si une menace est détectée dans un email

Lorsqu'un objet infecté est détecté dans une pièce jointe d'un *message sortant*, l'application empêche son envoi.

Si un objet infecté est détecté dans un *message entrant*, l'application peut tenter de désinfecter l'objet, puis soit supprimer l'objet, soit bloquer l'accès à celui-ci. Kaspersky Endpoint Security ajoute également des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

Lors de la configuration de la Protection contre les menaces par emails, vous pouvez sélectionner les actions que Kaspersky Endpoint Security exécutera en cas de détection d'une menace dans les messages électroniques.

Configuration des actions en cas de détection d'une menace dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces par emails**.

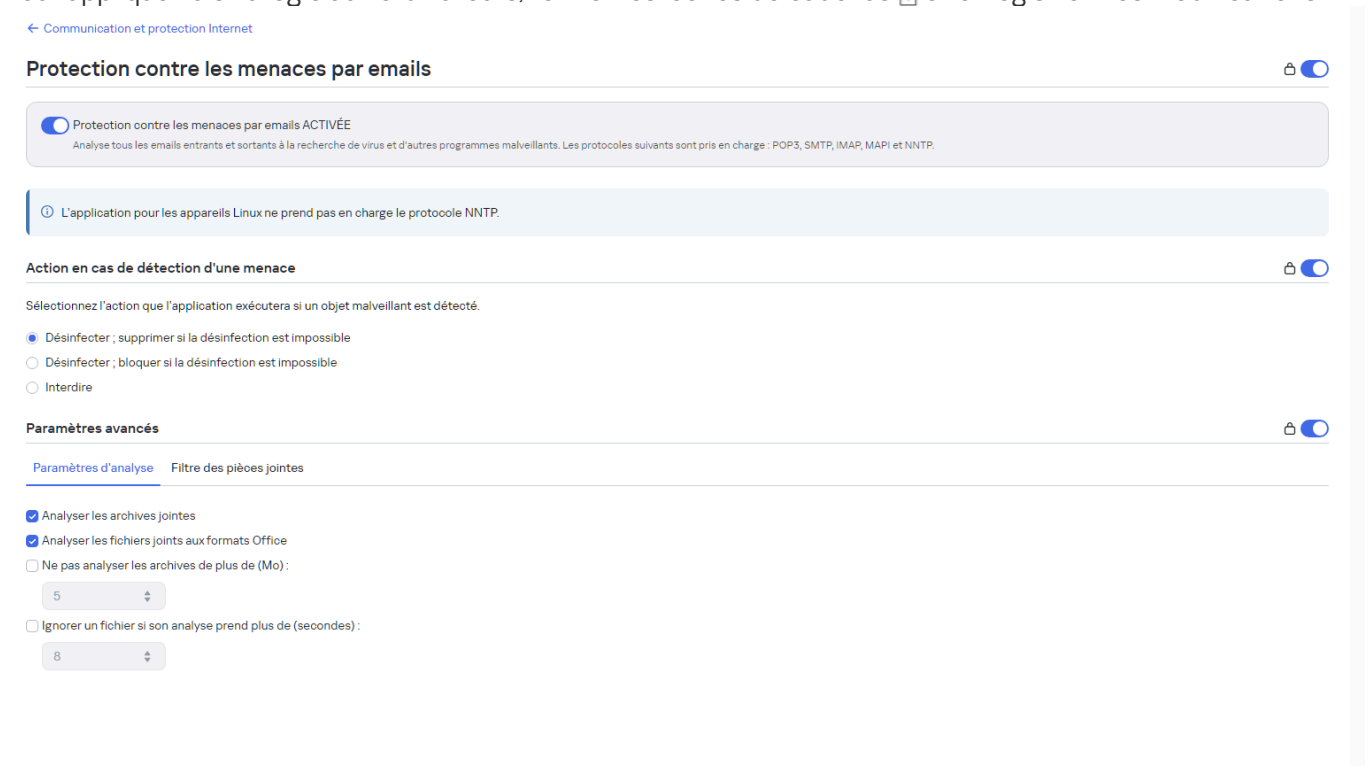
5. Sous **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera en cas de détection d'une menace :

   - **Désinfecter ; supprimer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

   - **Interdire**. Si un objet infecté est détecté dans un message entrant, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection contre les menaces par emails

Comment configurer les actions en cas de détection d'une menace via la ligne de commande

1. Assurez-vous que le module Protection contre les menaces par emails est activé :

   ```
   kesl-control --get-task-state 35
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

```
kesl-control --start-task 35
```

3. Sélectionnez une action à effectuer lorsqu'une menace par email est détectée dans les messages entrants :

```
kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

4. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 35
```

Symboles

Options de la commande

Paramètre	Description
`ActionOnThreat`	Action lors de la détection d'une menace : • `DisinfectDeleteIfNotPossible` (par défaut). Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur. • `DisinfectBlockIfNotPossible`. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur. • `Block`. Si un objet infecté est détecté dans un message entrant, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

Comment optimiser l'analyse des pièces jointes aux emails

Configurez l'analyse des pièces jointes aux emails afin d'optimiser le module Protection contre les menaces par emails. Cela permet de réduire l'utilisation du processeur sur l'appareil protégé. Vous pouvez limiter l'analyse des archives jointes, définir la taille maximale des pièces jointes pouvant être analysées et définir la durée maximale de l'analyse d'un objet.

Comment optimiser l'analyse des pièces jointes dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces par emails**.
5. Sous les **Paramètres avancés**, sélectionnez l'onglet **Paramètres d'analyse**.

6. Configurez l'analyse des pièces jointes :

   - **Analyser les archives jointes**. Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive).

   - **Analyser les fichiers joints aux formats Office**. Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. L'application analyse les fichiers au format Office de moins de 1 Mo, quel que soit l'état de la case.

   - **Ne pas analyser les archives de plus de (Mo)**. Si la case est cochée, le module Protection contre les menaces par emails exclut de l'analyse les archives jointes aux messages électroniques dont la taille dépasse celle spécifiée. Si cette case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques.

   - **Ignorer un fichier si son analyse prend plus de (secondes)**. Si la case est cochée, la durée d'analyse des archives jointes aux messages est limitée à la période spécifiée.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment optimiser l'analyse des pièces jointes en ligne de commande

1. Assurez-vous que le module Protection contre les menaces par emails est activé :

   ```
   kesl-control --get-task-state 35
   ```

2. Le module doit avoir l'état `Started`.

3. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 35
   ```

4. Sélectionnez une action à effectuer lorsqu'une menace par email est détectée dans les messages entrants :

   ```
   kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
   (MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
   ```

5. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

   ```
   kesl-control --get-settings 35
   ```

Symboles

Options de la commande

Paramètre	Description
`ScanFileArchive`	Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). Par défaut, l'application analyse les archives jointes.
`UseSizeLimit` `SizeLimit`	Limite la taille des archives jointes qui peuvent être analysées. Le module Protection contre les menaces par emails ignore une archive jointe lors de l'analyse si sa taille dépasse la valeur spécifiée. Par défaut, l'application analyse les archives de n'importe quelle taille.

Paramètre	Description
`UseTimeLimit` `TimeLimit`	Limite de temps pour l'analyse des archives jointes. Par défaut, le temps d'analyse des archives jointes n'est pas limité.
`ScanFileOffice`	Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. L'application analyse les fichiers au format Office de moins de 1 Mo, quel que soit l'état de la case. Par défaut, l'application analyse les fichiers au format Office joints.

À quoi sert un filtre des pièces jointes aux emails

Le filtre des pièces jointes ne s'applique pas aux emails sortants.

Les programmes malveillants peuvent se propager sous la forme des pièces jointes dans des messages électroniques. Vous pouvez configurer le filtrage selon le type des pièces jointes dans les messages de telle sorte qu'il soit possible de renommer ou de supprimer automatiquement les fichiers des types indiqués. En renommant une pièce jointe d'un type en particulier, Kaspersky Endpoint Security peut protéger votre ordinateur contre l'exécution d'un programme malveillant.

Par exemple, vous pouvez configurer le filtrage des pièces jointes pour les fichiers HTML. Un fichier HTML peut contenir des scripts malveillants. Si l'application renomme un tel fichier, l'utilisateur ne pourra pas ouvrir la page HTML en double-cliquant dessus dans un email. Pour ouvrir le fichier HTML, l'utilisateur devra télécharger le fichier et le renommer. Cela laisse à l'utilisateur le temps d'analyser le message reçu et d'empêcher le lancement du script malveillant.

Par défaut, l'application renomme les fichiers portant les extensions CMD, COM, EXE, JS, JSE, MSI, SCR, VBE, VBS et SH. L'application remplace le dernier caractère de l'extension des types de fichiers spécifiés par un trait de soulignement (par exemple, attachment.doc_).

Configuration du filtre des pièces jointes dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces par emails**.
5. Sous les **Paramètres avancés**, sélectionnez l'onglet **Filtre des pièces jointes**.

6. Sélectionnez l'action que l'application exécutera sur la pièce jointe à l'email :

   - **Ne pas modifier les pièces jointes**. Si cette option est sélectionnée, la Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques.

   - **Renommer les pièces jointes de types indiqués**. Lorsque cette option est sélectionnée, la Protection contre les menaces par emails remplace le dernier caractère de l'extension des fichiers joints des types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir.

   - **Supprimer les pièces jointes de types indiqués**. Lorsque cette option est sélectionnée, la Protection contre les menaces par emails supprime les pièces jointes des types de fichiers spécifiés des messages électroniques.

7. Si, à l'étape précédente, vous avez sélectionné l'option **Renommer les pièces jointes de types indiqués** ou **Supprimer les pièces jointes de types indiqués**, cochez les cases correspondant aux types de fichiers requis.

8. Si le type de fichier requis n'apparaît pas dans la liste, ajoutez un nouveau type de pièce jointe :

   a. Cliquez sur **Ajouter**.

      Le formulaire d'ajout d'un nouveau type de pièce jointe s'ouvre.

   b. Dans le champ **Types de pièces jointes**, indiquez les masques d'extension au format `*.<extension>` (par exemple, `*.doc`).

      Si vous souhaitez spécifier plusieurs types de fichiers, saisissez chaque type de fichier sur une nouvelle ligne.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration du filtre des pièces jointes via la ligne de commande

1. Assurez-vous que le module Protection contre les menaces par emails est activé :

```
kesl-control --get-task-state 35
```

2. Le module doit avoir l'état `Started`.

3. Si le module est désactivé, exécutez la commande suivante :

```
kesl-control --start-task 35
```

4. Sélectionnez l'action que l'application exécutera sur la pièce jointe à l'email :

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 35
```

Symboles

Options de la commande

Paramètre	Description
`ExtensionFilter`	Action que l'application exécutera sur la pièce jointe à l'email : `Disable`. Si cette option est sélectionnée, la Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques. `Rename` (par défaut). Lorsque cette option est sélectionnée, la Protection contre les menaces par emails remplace le dernier caractère de l'extension des fichiers joints des types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir. `Delete`. Lorsque cette option est sélectionnée, la Protection contre les menaces par emails supprime les pièces jointes des types de fichiers spécifiés des messages électroniques.
`UseExtensionMask=Yes`	Ajout d'un type de fichier au filtre des pièces jointes. Vous pouvez exclure temporairement un type de fichier du filtre des pièces jointes au lieu de le supprimer. Pour ce faire, définissez `ExtensionMasks.item_#.UseExtensionMask=No`
`ExtensionMasks=*.<extention>`	Extension du type de pièce jointe que vous souhaitez renommer ou supprimer des emails.

Protection contre les menaces Internet

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants depuis Internet et bloque également la connexion aux sites Internet malveillants et de phishing. Le module protège l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et d'une analyse heuristique.

Fonctionnement de la Protection contre les menaces Internet

Lors de l'installation de Kaspersky Endpoint Security, l'application ajoute un certificat auto-signé, *Certificat racine personnel de Kaspersky Anti-Virus*. L'application place ce certificat dans le magasin local de certificats de confiance (`/etc/ssl/certs`) et dans le magasin de certificats des navigateurs Internet. À chaque démarrage, l'application vérifie la présence du certificat. Si le certificat a été supprimé, l'application le restaure automatiquement.

1. **Interception d'une connexion sortante**

   Une application tierce (par exemple, un navigateur) initie une connexion à un serveur. Kaspersky Endpoint Security remplace le certificat du serveur par son propre certificat signé avec le Certificat racine personnel de Kaspersky Anti-Virus. Ensuite, l'application intercepte la clé de chiffrement et déchiffre la session de communication. Kaspersky Endpoint Security effectue cette opération sans alerter l'utilisateur, car le Certificat racine personnel de Kaspersky Anti-Virus se trouve dans le magasin de certificats de confiance.

2. **Analyse du trafic réseau**

   La Protection contre les menaces Internet analyse le trafic à l'aide des technologies suivantes :

   - Bases antivirus.
   - Services cloud de Kaspersky Security Network.
   - La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

3. **Fin de l'analyse**

   Si un site Internet est classé comme site malveillant ou de phishing, Kaspersky Endpoint Security exécute l'action indiquée dans les paramètres du module Protection contre les menaces Internet : il bloque la connexion ou affiche un avertissement.

Paramètres du module Protection contre les menaces Internet

1. **Configurer les règles du pare-feu du système d'exploitation**

   Si le système dispose de ses propres règles réseau ou de règles firewalld avec des stratégies Drop, alors pour que l'application fonctionne correctement, vous devez ajouter une règle autorisant les connexions entrantes depuis l'appareil local (loopback) :

   Exemple de la commande pour iptables :

   ```
   iptables -A INPUT -i lo -j ACCEPT
   ```

2. **Sélectionner le mode d'interception du trafic réseau**

   À la réception des paquets réseau, la Protection contre les menaces Internet extrait les données afin de les analyser à la recherche de menaces. Les modes suivants d'interception du trafic réseau peuvent être utilisés :

   - eBPF
   - iptables (par défaut)

   Le choix du mode d'interception du trafic réseau dépend de l'infrastructure de l'entreprise. Dans un périmètre fermé, nous recommandons d'utiliser eBPF. Dans les autres scénarios, utilisez iptables.

   > Nous recommandons de regrouper les appareils dans différents groupes d'administration en fonction du mode d'interception du trafic réseau.

3. **Configurer la stratégie de validation des certificats**

   Par défaut, la Protection contre les menaces Internet déchiffre et analyse le trafic réseau transmis via des connexions chiffrées. Dans ce cas, le module peut utiliser Internet pour vérifier et télécharger les chaînes manquantes nécessaires à la vérification du certificat. Si l'appareil n'a pas d'accès direct à Internet, vous devez sélectionner une méthode locale de validation des certificats (sans utiliser Internet) ou utiliser un serveur proxy pour accéder à Internet.

   La stratégie de validation des certificats inclut également les paramètres suivants :

   - Accès aux sites Internet avec un certificat non fiable
   - Accès aux sites Internet avec une erreur de validation du certificat

   Par défaut, Kaspersky Endpoint Security autorise l'accès à un site Internet avec un certificat non fiable et ajoute aux exclusions le domaine présentant une erreur de validation du certificat. Des erreurs de validation du certificat peuvent survenir, par exemple, lors de l'utilisation d'applications bancaires ou d'un stockage dans le cloud. Les domaines auxquels ces services appartiennent peuvent rejeter le certificat racine personnel de Kaspersky Anti-Virus. Vous pouvez configurer votre propre stratégie de validation des certificats.

4. **Ajouter des certificats de confiance**

   Si votre organisation utilise des autorités de certification privées pour émettre des certificats pour des serveurs internes, Kaspersky Endpoint Security peut bloquer l'accès aux ressources Internet en raison d'erreurs de validation des certificats. Ajoutez ces certificats à la liste de confiance afin d'exclure les ressources Internet de l'analyse des connexions chiffrées.

5. **Dans les paramètres de la Protection contre les menaces Internet, sélectionnez l'action Informer**

   Par défaut, la pProtection contre les menaces Internet est désactivée. Nous vous recommandons d'activer la Protection contre les menaces Internet et, comme action lors de la détection d'une menace, de sélectionner **Informer**, puis de vérifier l'accès à toutes les ressources de l'entreprise. Kaspersky Endpoint Security autorise l'accès à tous les sites Internet et consigne les informations relatives aux menaces détectées.

6. **Collecter des statistiques sur les sites Internet que la Protection contre les menaces Internet considère comme dangereux**

   Vous pouvez obtenir des statistiques sur les sites Internet que la Protection contre les menaces Internet considère comme dangereux à l'aide de rapports.

7. **Ajouter des adresses Internet de confiance**

   Après avoir examiné les rapports de la Protection contre les menaces Internet, vous devez ajouter les adresses Internet auxquelles vous faites confiance à la liste de confiance. Si la liste des adresses Internet de confiance ne suffit pas à résoudre le conflit entre l'application Kaspersky Endpoint Security et des applications tierces, vous pouvez utiliser la chaîne spéciale de règles d'autorisation kesl_bypass. La *chaîne kesl_bypass* est une liste spéciale de règles que Kaspersky Endpoint Security crée dans la table mangle du Firewall du système d'exploitation (iptables/ip6tables).

8. **Dans les paramètres de la Protection contre les menaces Internet, sélectionnez l'action Bloquer**

   Activez le blocage des objets infectés dans le trafic Internet.

Considérations particulières et limitations

- L'application analyse le trafic entrant sur les ports TCP et utilise le port 9879 sur localhost pour intercepter les connexions. Si le port 9879 est utilisé, l'application sélectionne automatiquement un port disponible pour intercepter les connexions.
- L'activation ou la désactivation de l'application, ainsi que l'activation ou la désactivation des modules Protection contre les menaces Internet et Protection contre les menaces réseau, met fin aux connexions sur les ports interceptés.
- Kaspersky Endpoint Security analyse le trafic HTTP et HTTPS. Kaspersky Endpoint Security analyse les adresses Internet et IP.
- L'application prend en charge les fichiers exécutables de navigateurs suivants, y compris au format snap :
  - chrome ;
  - chromium ;
  - chromium-browser ;
  - firefox ;
  - firefox-esr ;
  - google-chrome ;
  - opera ;
  - yandex-browser.

- Si un utilisateur tente d'accéder à un site Internet malveillant, l'application effectue les actions suivantes :
  - **HTTP**. L'application bloque l'accès et affiche un avertissement.
  - **HTTPS**. L'application bloque l'accès ; le navigateur affiche une page d'erreur.
- La suppression des certificats de l'application peut entraîner un fonctionnement incorrect du module de protection contre les menaces Internet.

Articles utiles

Que faire si vous recevez l'avertissement « Visite d'un domaine avec un certificat non fiable »

Comment sélectionner une action lors de la détection d'une menace Internet

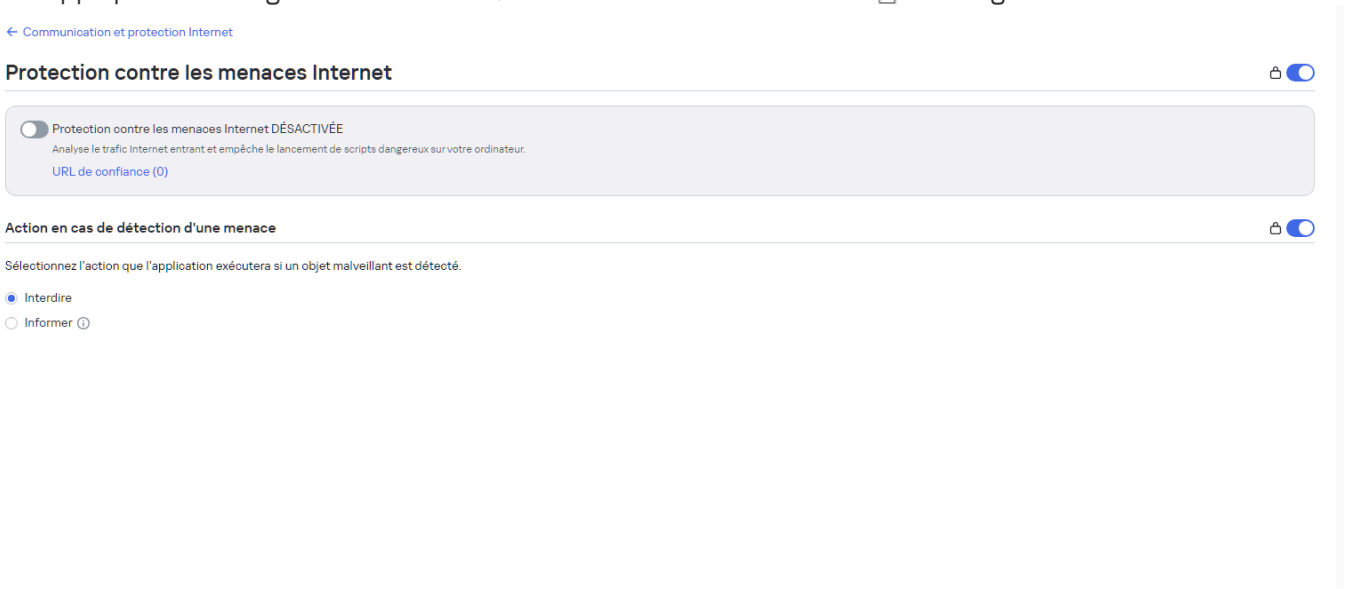
En cas de détection d'une menace Internet, Kaspersky Endpoint Security peut bloquer l'accès aux objets dangereux ou uniquement informer de la détection d'un objet dangereux.

Comment configurer les actions en cas de détection d'une menace Internet dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces Internet**.
5. Sous **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera en cas de détection d'une menace :
   - **Interdire**. Si cette action est sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche un message dans le navigateur.
   - **Informer**. Kaspersky Endpoint Security informe l'utilisateur de la détection d'un objet infecté dans le trafic Internet. La Protection contre les menaces Internet autorise le téléchargement de cet objet sur l'appareil. À ce stade, l'application enregistre les informations relatives à l'objet infecté et ajoute celui-ci à la liste des menaces actives.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection contre les menaces Internet

Comment configurer les actions en cas de détection d'une menace via la ligne de commande

1. Exécutez la commande:

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. Sélectionnez les bases de données à utiliser pour l'analyse des liens :

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 14
```

Symboles

Options de la commande

Paramètre	Description
`ActionOnDetect`	Action lors de la détection d'une menace : • `Block` (par défaut). Si cette action est sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche un message dans le navigateur. • `Notify`. Si cette option est sélectionnée, Kaspersky Endpoint Security permet, en cas de détection d'un objet infecté dans le trafic Internet, de télécharger cet objet sur l'ordinateur et ajoute les informations sur l'objet infecté à la liste des menaces actives.
`CheckMalicious`	L'analyse des liens pour déterminer s'ils sont inclus dans la base de données des adresses Internet malveillantes vous permet de suivre les sites Internet qui ont été ajoutés à la liste de refus. La base des adresses Internet malveillantes est créée par les experts de Kaspersky. Elle est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security. L'analyse est activée par défaut (`Yes`).
`CheckAdware`	Vérification des liens par rapport à la base de données des adresses Internet publicitaires. L'analyse est désactivée par défaut (`No`).
`CheckOther`	Vérification des liens par rapport à la base de données d'adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données. L'analyse est désactivée par défaut (`No`).

Qu'est-ce que l'Antihameçonnage

La Protection contre les menaces Internet vérifie les liens pour vérifier s'ils appartiennent à des adresses Internet de phishing. Cette mesure permet d'éviter les *attaques de phishing*. L'exemple type en est le message électronique prétendument envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel de la banque. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site Internet de phishing peut figurer non seulement dans un message électronique, mais également dans d'autres sources, comme des messageries, le module Protection contre les menaces Internet contrôle les tentatives d'accès à un site de phishing au niveau de l'analyse du trafic Internet et bloque l'accès à ces sites Internet. La liste des adresses de phishing est reprise dans la distribution de Kaspersky Endpoint Security.

Vous pouvez configurer la fonctionnalité Anti-phishing uniquement via la ligne de commande. Vous ne pouvez pas configurer l'Anti-phishing dans Web Console. Par défaut, l'Anti-Phishing avec analyse heuristique est activé.

Comment activer l'Anti-phishing via la ligne de commande

1. Assurez-vous que le module Protection contre les menaces Internet est activé :

   ```
   kesl-control --get-task-state 14
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 14
   ```

3. Activer l'Anti-phishing :

   ```
   kesl-control --set-settings 14 CheckPhishing=Yes
   ```

4. Configurez l'analyse heuristique pour rechercher des liens de phishing sur les pages Internet :

   ```
   kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
   ```

   Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.

5. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

   ```
   kesl-control --get-settings 14
   ```

Protection contre les menaces réseau

Le module *Protection contre les menaces réseau* (également appelé Intrusion Detection System, IDS) surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, l'application bloque la connexion réseau issue de l'ordinateur attaquant. Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de l'application. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la mise à jour des bases et des modules de l'application.

Fonctionnement de la Protection contre les menaces réseau

1. **L'application analyse les paquets entrants**

   Pour analyser le trafic entrant, le module Protection contre les menaces réseau reçoit les numéros de port des bases de données de l'application et accepte les connexions via tous ces ports. Lors du processus d'analyse du réseau en mode d'interception du trafic iptables, cela peut donner l'impression qu'un port est ouvert sur l'appareil, même si aucune application du système n'est à l'écoute sur ce port. Nous recommandons de fermer les ports inutilisés à l'aide d'un pare-feu.

2. **L'application analyse le trafic entrant**

   La Protection contre les menaces réseau analyse le trafic entrant à l'aide des technologies suivantes :

   - Bases antivirus.
   - Services cloud de Kaspersky Security Network.
   - La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

3. **Fin de l'analyse**

   Lorsqu'une menace réseau est détectée, l'application bloque toutes les connexions réseau provenant de l'appareil attaquant pendant une durée définie.

Paramètres de la Protection contre les menaces réseau

1. **Configurer les règles du pare-feu du système d'exploitation**

   Pour garantir la compatibilité des règles REDIRECT (par exemple, la redirection du port 443 vers le port 8443) avec les règles d'interception de la Protection contre les menaces réseau, vous devez supprimer les règles REDIRECT et ajouter des règles d'interception.

   Exemple de commande permettant de supprimer les règles REDIRECT :

   ```
   iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

   Exemple de commandes permettant d'ajouter des règles d'interception :

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
   ```

   ```
   iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT --to-destination :8443
   ```

2. **Créer une liste de ports réseau contrôlés**

   Par défaut, l'application contrôle les ports connus et enregistrés, par exemple le port 443 pour les connexions HTTPS et le port 143 pour le protocole de messagerie IMAP. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources. Si nécessaire, vous pouvez modifier la liste des ports contrôlés ou activer le contrôle de tous les ports.

3. **Sélectionner le mode d'interception du trafic**

   À la réception de paquets réseau, la Protection contre les menaces réseau extrait les données afin de rechercher des menaces. Les modes suivants peuvent être utilisés pour l'interception du trafic entrant :

   - eBPF
   - iptables (par défaut)

   Le choix du mode d'interception du trafic dépend de l'infrastructure de l'organisation. Dans un périmètre fermé, nous recommandons d'utiliser eBPF. Dans les autres scénarios, utilisez iptables.

   > Nous recommandons de regrouper les appareils dans différents groupes d'administration en fonction du mode d'interception du trafic.

4. **Activer la Protection contre les menaces Internet en mode Information**

   Par défaut, la Protection contre les menaces réseau est désactivée. Avant d'activer la Protection contre les menaces réseau en mode Blocage, nous vous recommandons d'activer le module en mode Information. Cela permet à Kaspersky Endpoint Security de détecter toute activité réseau suspecte et de consigner les informations relatives aux attaques réseau détectées sans interrompre les connexions réseau. Vérifiez l'accès des applications d'entreprise tierces aux ressources réseau. Assurez-vous que le contrôle des ports réseau ne ralentit pas ces applications.

5. **Collecter des statistiques sur les adresses IP depuis lesquelles la Protection contre les menaces réseau détecte une activité réseau suspecte**

   Vous pouvez consulter les rapports pour obtenir des statistiques sur les adresses IP que la Protection contre les menaces réseau considère comme dangereuses. L'application génère des événements *Une attaque réseau a été détectée*.

6. **Ajouter des adresses IP de confiance**

   Après avoir consulté les rapports de la Protection contre les menaces réseau, vous devez ajouter à la liste de confiance les adresses IP des appareils dont vous considérez les connexions réseau comme fiables. Vous pouvez ajouter l'adresse d'un appareil individuel ou d'un sous-réseau à la liste des exclusions. La Protection contre les menaces réseau n'intercepte pas et n'analyse pas les paquets provenant d'un tel appareil.

7. **Activer la Protection contre les menaces réseau en mode Blocage**

   Après avoir ajouté les adresses IP des appareils de confiance à la liste des exclusions, activez le module en mode Blocage. L'activité réseau des appareils non fiables est bloquée et les informations correspondantes apparaissent dans les rapports.

Considérations particulières et limitations

- L'application analyse le trafic entrant sur les ports TCP. L'application utilise le port fixe 9789 sur localhost pour intercepter les connexions.
- L'activation ou la désactivation de l'application, ainsi que l'activation ou la désactivation des modules Protection contre les menaces Internet et Protection contre les menaces réseau, met fin aux connexions sur les ports interceptés.
- La Protection contre les menaces réseau ne fonctionne pas sur les ordinateurs exécutant CentOS 5.2 et 5.4 en raison de l'absence de prise en charge de TProxy.

Comment sélectionner une action lors de la détection d'une menace réseau

En cas de détection d'une tentative d'attaque réseau contre un appareil protégé, l'application bloque l'activité réseau de l'appareil à l'origine de l'attaque et crée un événement *Une attaque réseau a été détectée*.

Pour bloquer le trafic réseau, Kaspersky Endpoint Security crée une règle de pare-feu dynamique. Le pare-feu bloque temporairement le trafic réseau de l'appareil attaquant. L'application ajoute également l'appareil compromis à la liste des appareils bloqués. L'accès aux répertoires réseau partagés est refusé aux appareils bloqués.

Configuration des actions en cas de détection d'une attaque réseau dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces réseau**.

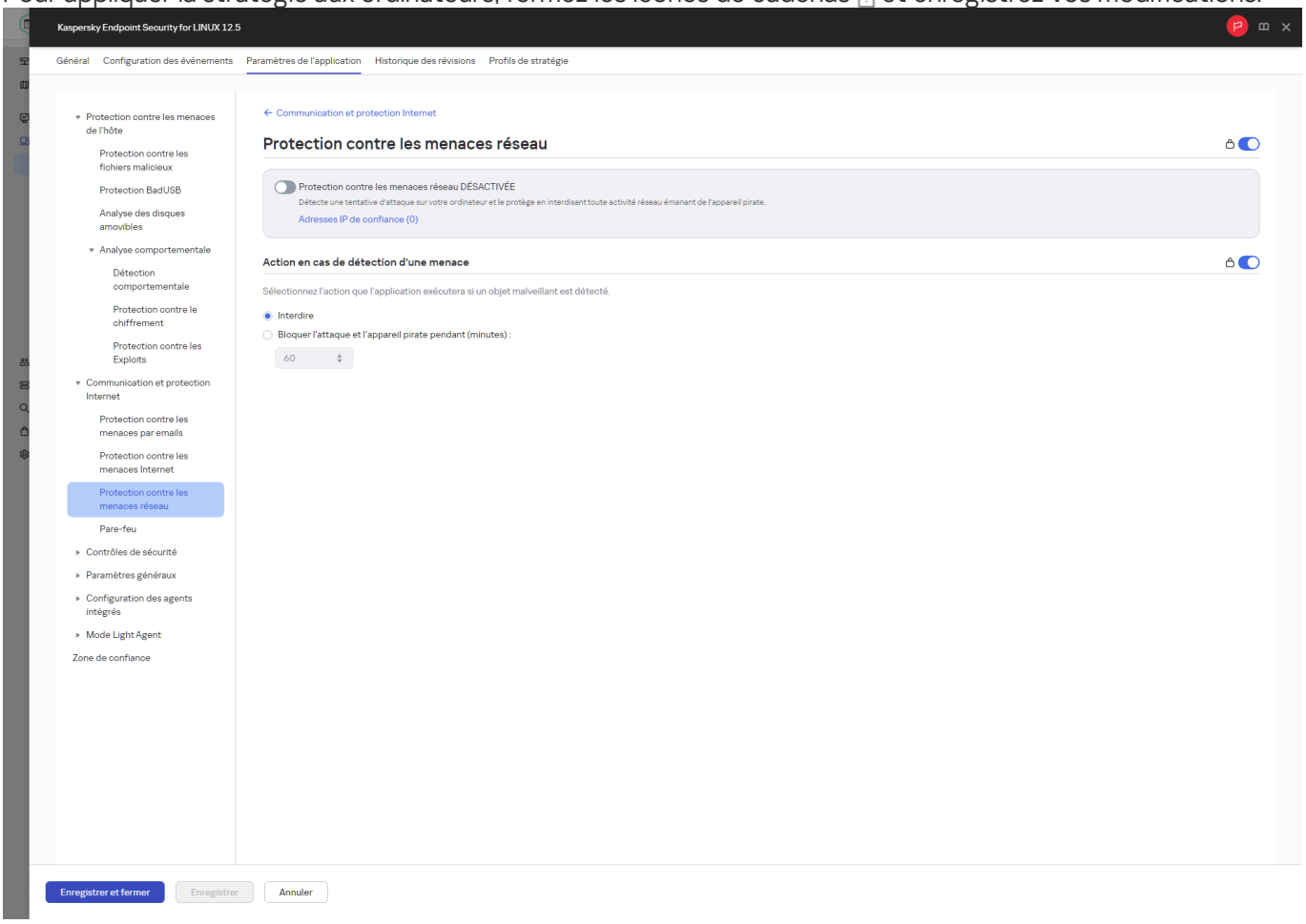
5. Assurez-vous que le commutateur du module est en position **Protection contre les menaces réseau ACTIVÉE**.

6. Cochez la case **Activer la protection contre les menaces réseau pour les appareils Linux**.

7. Sous **Action en cas de détection d'une menace**, sélectionnez l'action que l'application exécutera lorsqu'une menace est détectée : **Interdire** ou **Bloquer l'attaque et l'appareil pirate pendant (minutes)**.

8. Si **Bloquer l'attaque et l'appareil pirate pendant (minutes)** est sélectionné, définissez la durée de blocage de l'appareil compromis en minutes. Par défaut, l'appareil est bloqué pendant 60 minutes. Les valeurs valides sont de 1 à 999.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Protection contre les menaces réseau

Configuration des actions en cas de détection d'une attaque réseau via la ligne de commande

1. Assurez-vous que le module Protection contre les menaces réseau est activé :

```
kesl-control --get-task-state 17
```

Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

```
kesl-control --start-task 17
```

3. Sélectionnez une action en cas de détection d'une menace réseau :

```
kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
```

4. Configurez le blocage de l'appareil compromis :

```
kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
```

5. Sélectionnez la durée de blocage pour l'action `BlockAttackingHosts=Yes` :

```
kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
```

6. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 17
```

Symboles

Options de la commande

Paramètre	Description
`ActionOnDetect`	Action en cas de détection d'une menace réseau : • `Block` (par défaut) bloque le trafic réseau de l'appareil compromis et crée un événement *Une attaque réseau a été détectée*. • `Notify` crée un événement *Une attaque réseau a été détectée* sans bloquer le trafic réseau.
`BlockAttackingHosts`	Bloquez l'activité réseau de l'appareil attaquant. Par défaut, le blocage des appareils est activé.
`BlockDurationMinutes`	Configurez la durée de blocage de l'appareil distant impliqué dans une activité malveillante ou un chiffrement malveillant des données.

Comment gérer les appareils bloqués

Tout en protégeant un appareil contre les menaces réseau et contre le chiffrement malveillant à distance, Kaspersky Endpoint Security peut bloquer les appareils distants dont les actions sont considérées comme malveillantes. Les appareils sont protégés contre les menaces de ces types par les modules Protection contre le chiffrement et Protection contre les menaces réseau. Kaspersky Endpoint Security bloque le trafic réseau pendant une certaine durée. À l'expiration de la période de blocage, Kaspersky Endpoint Security autorise la reprise du trafic réseau. Par défaut, l'application bloque le trafic réseau d'un appareil attaquant pendant 60 minutes. À l'expiration de la durée de blocage, l'application supprime cet appareil de la liste des appareils bloqués.

Si Kaspersky Endpoint Security a bloqué un appareil de confiance, vous devez ajouter l'adresse IP de cet appareil à la liste des exclusions.

Comment consulter la liste des appareils bloqués

```
kesl-control -H --get-blocked-hosts
```

À la suite de l'exécution de la commande, l'application affiche une liste des appareils bloqués sur la console.

Liste des appareils bloqués

```
Blocked devices: 1
Host               : 10.69.119.234
```

```
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

Comment débloquer un appareil

```
kesl-control -H --allow-hosts <address>
```

Où `<address>` correspond à une ou plusieurs adresses IP des appareils ou des sous-réseaux (IPv4/IPv6, y compris les adresses abrégées). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

Gestion du pare-feu

Le pare-feu du système d'exploitation contrôle toute l'activité réseau de l'appareil, qu'il s'agisse de l'activité sur Internet ou sur le réseau local. Le pare-feu protège les données de l'appareil contre les accès non autorisés et bloque la plupart des menaces, par exemple les attaques contre l'appareil provenant du réseau. Le pare-feu permet de détecter toutes les connexions réseau sur l'appareil de l'utilisateur et d'obtenir la liste de leurs adresses IP.

L'application gère le pare-feu du système d'exploitation à l'aide du module Gestion du pare-feu. Le module ajoute des règles pour les paquets réseau au pare-feu du système d'exploitation afin de surveiller l'activité réseau des appareils. À l'aide des règles de paquets réseau, vous pouvez définir le niveau souhaité de protection de l'appareil, du blocage complet de l'accès Internet pour toutes les applications à l'autorisation d'un accès illimité.

Par défaut, le module Gestion du pare-feu est désactivé.

Lorsque vous activez le module Gestion du pare-feu, Kaspersky Endpoint Security supprime automatiquement toutes les règles utilisateur configurées pour le pare-feu à l'aide du système d'exploitation. Après désactivation du module, ces règles ne sont pas restaurées.

Si la Gestion du pare-feu est activée, Kaspersky Endpoint Security vérifie le pare-feu du système d'exploitation toutes les 60 secondes. Si la vérification révèle qu'une application ou qu'un utilitaire tiers a ajouté ou supprimé une règle pour les paquets réseau, Kaspersky Endpoint Security restaure l'ensemble de règles du pare-feu créé à l'aide de l'application.

Kaspersky Endpoint Security vérifie toujours le pare-feu du système d'exploitation lorsque la gestion du pare-feu est désactivée. Cela permet à l'application de rétablir les règles dynamiques.

Avant d'activer le module Gestion du pare-feu, effectuez les actions suivantes :

- Désactivez les autres outils qui gèrent le pare-feu du système d'exploitation.
- Enregistrez et sauvegardez toutes les règles personnalisées du pare-feu configurées avant l'activation du module Gestion du pare-feu.

Création d'une règle pour les paquets réseau

Le pare-feu filtre toute l'activité réseau sur les appareils protégés conformément aux *règles pour les paquets réseau*. Les règles pour les paquets réseau limitent les paquets réseau ou les connexions, indépendamment de l'application. Les règles autorisent ou interdisent l'activité réseau selon les conditions suivantes :

- Protocole et port de connexion
- Direction du trafic
- Adresse IP de l'appareil qui envoie ou reçoit du trafic réseau

Priorités des règles pour les paquets réseau

Par défaut, tous les paquets et toutes les connexions sortants. Les règles par défaut ont la priorité la plus faible : si aucune autre règle pour les paquets réseau n'a été déclenchée ou si aucune autre règle pour les paquets réseau n'a été définie, l'activité est autorisée.

Le pare-feu applique les règles pour les paquets réseau dans l'ordre de leur priorité. La priorité d'une règle correspond à sa position dans la liste, de haut en bas. Le pare-feu filtre une connexion réseau selon la première règle de la liste et autorise ou bloque l'activité réseau. Si la règle ne correspond pas, le pare-feu applique la règle suivante, et ainsi de suite jusqu'en bas de la liste. Le module ignore alors toutes les règles pour les paquets réseau qui suivent la règle correspondant à la connexion.

Recommandations pour la création de règles pour les paquets réseau

Pour créer des règles de paquet réseau en ligne de commande, vous pouvez utiliser les options de ligne de commande ou un fichier de configuration. Si vous souhaitez ajouter plusieurs règles, utilisez un fichier de configuration pour les ajouter.

L'ajout d'un grand nombre de règles une par une à l'aide des options de ligne de commande peut provoquer un pic de charge du processeur.

Comment créer une règle pour les paquets réseau dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.
5. Assurez-vous que le commutateur du module est en position **Pare-feu ACTIVÉ**.

6. Sous l'onglet **Règles pour les paquets réseau**, cliquez sur le bouton **Ajouter**.

   Le formulaire de création d'une règle réseau s'ouvre (voir la figure ci-dessous).

7. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Sélectionner un modèle de règle**. Les modèles de règles contiennent des paramètres pour les connexions réseau les plus fréquemment utilisées.

   Tous les paramètres d'une règle réseau, à l'exception de la priorité et des actions que le pare-feu applique à la connexion, sont renseignés automatiquement.

8. Dans le champ **Priorité**, indiquez la priorité de la règle. Par défaut, une règle est créée avec la priorité la plus élevée.

9. Sous **Action**, sélectionnez la manière dont le pare-feu doit traiter l'activité réseau lorsque la règle est déclenchée : **Autoriser** ou **Interdire**.

10. Dans le champ **Direction**, sélectionnez l'activité réseau à laquelle vous souhaitez appliquer la règle :

    - **Entrant**. Le pare-feu applique la règle réseau à tous les paquets réseau entrants.
    - **Entrant (paquet)**. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par un ordinateur distant.
    - **Entrant/Sortant**. Le pare-feu applique la règle réseau aux paquets réseau entrants et sortants, quel que soit l'ordinateur (l'ordinateur de l'utilisateur ou l'ordinateur distant) qui a amorcé la connexion réseau.
    - **Sortant (paquet)**. Le pare-feu applique la règle réseau à tous les paquets réseau sortants.
    - **Sortant**. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par l'ordinateur de l'utilisateur.
    - **Paquets entrants/sortants**. Le pare-feu applique la règle réseau à tous les paquets réseau entrants et sortants.

11. Cochez la case **Consigner dans le rapport** si vous souhaitez que les actions de la règle réseau soient consignées dans le rapport. En fonction de l'action de la règle, l'application crée un événement *L'activité réseau est interdite* ou *L'activité réseau est autorisée*.

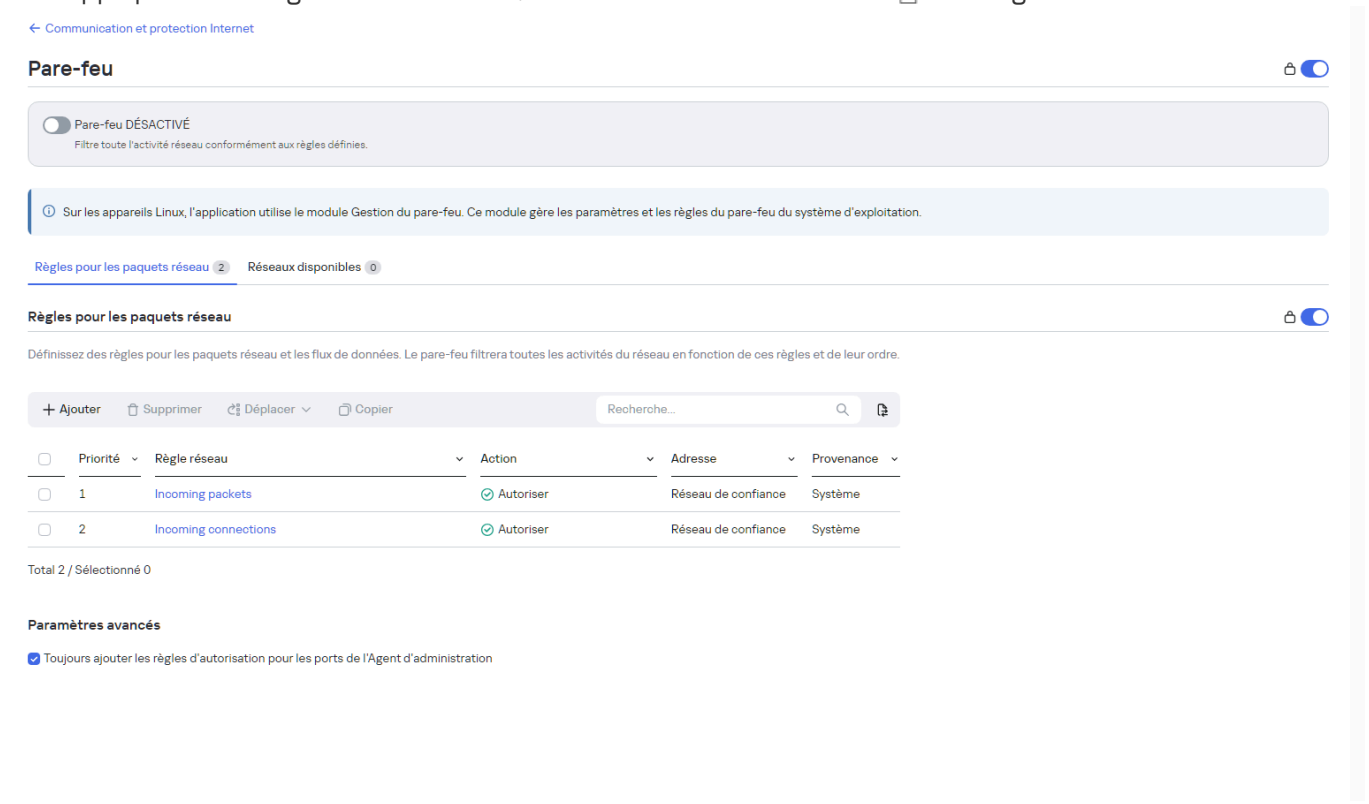
12. Sous l'onglet **Paramètres du protocole**, sélectionnez le protocole pour lequel vous souhaitez que la règle filtre l'activité réseau.

13. Rendez-vous dans l'onglet **Adresses des réseaux distants**.

14. Dans le champ **À distance**, indiquez les adresses réseau des ordinateurs distants qui peuvent envoyer et recevoir des paquets réseau : le pare-feu appliquera la règle aux adresses indiquées.

15. Dans le champ **Local**, indiquez les adresses réseau des ordinateurs sur lesquels Kaspersky Endpoint Security est installé et qui peuvent envoyer et recevoir des paquets réseau : le pare-feu appliquera la règle aux adresses indiquées.

16. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Pare-feu

Comment créer une règle pour les paquets réseau via la ligne de commande

1. Assurez-vous que la Gestion du pare-feu est activée :

   ```
   kesl-control --get-task-state 12
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 12
   ```

3. Ajoutez une nouvelle règle pour les paquets réseau :

   ```
   kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
   <direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
   ```

   Si vous souhaitez ajouter plusieurs règles, utilisez un fichier de configuration pour les ajouter :

   a. Exportez les paramètres du module dans le fichier de configuration :

      ```
      kesl-control --get-settings 12 --file <path to file> [--json]
      ```

b. Ouvrez le fichier de configuration et ajoutez des règles de paquet réseau avec les sections suivantes :

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. Importez les paramètres du fichier de configuration dans l'application :

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. Pour afficher la liste des règles pour les paquets réseau, exécutez la commande suivante :

```
kesl-control -F --query
```

L'application affiche la liste de toutes les règles pour les paquets réseau au format suivant : `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`.

Symboles

Options de la commande

Paramètre	Description
`--name <rule name>` `Name`	Le nom de la règle de paquet réseau. Par défaut, `Packet rule #<n>`.
`--action` `FirewallAction`	Action à réaliser sur les connexions définies dans cette règle de paquet réseau. • `Allow` (par défaut) pour autoriser les connexions. • `Block` pour bloquer les connexions.
`--protocol` `Protocol`	Type de protocole pour lequel vous souhaitez contrôler l'activité réseau. • `Any` (par défaut) signifie que le pare-feu contrôle toute l'activité réseau • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`
`--direction` `Direction`	Direction de l'activité réseau contrôlée : • `IncomingOutgoing` ou `InOut` (par défaut). Le pare-feu applique la règle réseau à tous les paquets réseau entrants et sortants. • `Incoming` ou `In`. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par un ordinateur distant. • `Outgoing` ou `Out`. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par l'ordinateur de l'utilisateur. • `IncomingPacket` ou `InPacket`. Le pare-feu applique la règle réseau à tous les paquets réseau entrants. • `OutgoingPacket` ou `OutPacket`. Le pare-feu applique la règle réseau à tous les paquets réseau sortants. • `IncomingOutgoingPacket` ou `InOutPacket`. Le pare-feu applique la règle réseau aux paquets réseau entrants et sortants, quel que soit l'ordinateur (l'ordinateur de l'utilisateur ou l'ordinateur distant) qui a amorcé la connexion réseau.

Paramètre	Description
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	Adresse IP de l'appareil distant : • `Any` (par défaut) permet de contrôler les paquets réseau envoyés et/ou reçus par des appareils distants avec n'importe quelle adresse IP. • `Trusted` est la zone réseau configurée pour les réseaux de confiance. • `Local` est la zone réseau configurée pour les réseaux locaux. • `Public` est la zone réseau configurée pour les réseaux publics. • `d.d.d.d` est l'adresse IPv4, où d est un nombre décimal compris entre 0 et 255. • `d.d.d.d – d.d.d.d` est une plage d'adresses IPv4. • `d.d.d.d/p` est un sous-réseau IPv4, où `p` est un nombre compris entre 0 et 32. • `x:x:x:x:x:x:x:x` est l'adresse IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` est une plage d'adresses IPv6. • `x:x:x:x:x:x:x:x/p` est le sous-réseau d'adresses IPv6, où `p` est un nombre compris entre 0 et 128 ; vous pouvez utiliser `::` pour plus de concision. Vous pouvez également spécifier un port distant : • `Any` (par défaut) pour contrôler tous les ports distants • `0 – 65535`.
`--local <local address[:<port>]>` `LocalAddress=<local address>`	Adresse réseau d'un appareil sur lequel l'application Kaspersky Endpoint Security est installée : • `Any` (par défaut) pour contrôler les paquets réseau envoyés et/ou reçus par des appareils locaux possédant n'importe quelle adresse IP. • `Trusted` est la zone réseau configurée pour les réseaux de confiance. • `Local` est la zone réseau configurée pour les réseaux locaux. • `Public` est la zone réseau configurée pour les réseaux publics. • `d.d.d.d` est l'adresse IPv4, où d est un nombre décimal compris entre 0 et 255. • `d.d.d.d – d.d.d.d` est une plage d'adresses IPv4. • `d.d.d.d/p` est un sous-réseau IPv4, où `p` est un nombre compris entre 0 et 32. • `x:x:x:x:x:x:x:x` est l'adresse IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` est une plage d'adresses IPv6. • `x:x:x:x:x:x:x:x/p` est le sous-réseau d'adresses IPv6, où `p` est un nombre compris entre 0 et 128 ; vous pouvez utiliser `::` pour plus de concision. Vous pouvez également spécifier un port local : • `Any` (par défaut) pour contrôler tous les ports locaux • `0 – 65535`.
`--at <index>`	Index de la règle dans la liste des règles de paquets réseau. Si le commutateur `--at` n'est pas spécifié ou si sa valeur est supérieure au nombre de règles dans la liste, la nouvelle règle est ajoutée à la fin de la liste.
`LogAttempts`	Incluez un enregistrement dans le rapport d'action des règles de réseau. • `Yes` : enregistrer les actions dans un rapport. • `No` (valeur par défaut) : ne pas enregistrer les actions dans un rapport.

Exemple de règle qui bloque toutes les connexions entrantes et établies au port TCP 23

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

Exemple de règle qui bloque les connexions entrantes et établies via le port TCP 23 pour la zone réseau Public

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

Exemples d'utilisation de règles pour les paquets réseau

1. **Autoriser l'accès à Internet uniquement pour un ordinateur spécifique du réseau local et bloquer l'accès pour tous les autres**

   Règle pour un ordinateur (192.168.2.22) autorisé à accéder à Internet via le protocole TCP :

   ```
   kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
   ```

   Règle pour les autres ordinateurs dont l'accès à Internet est bloqué :

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
   ```

2. **Bloquer l'accès à Internet uniquement pour un ordinateur spécifique du réseau local**

   Règle pour l'ordinateur (192.168.2.23) dont l'accès à Internet est bloqué :

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
   ```

3. **Bloquer l'accès à un site Internet spécifique depuis le réseau local**

   Règle pour les ordinateurs du réseau local auxquels l'accès HTTP à example.com (91.198.174.192) est refusé :

   ```
   kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
   ```

   Règle pour les ordinateurs du réseau local auxquels l'accès HTTPS à example.com (91.198.174.192) est refusé :

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
   ```

4. **Autoriser l'accès à un seul site Internet spécifié pour un ordinateur spécifique du réseau local**

   Règle pour un ordinateur (192.168.2.24) autorisé à accéder via HTTP à example.com (91.198.174.192) :

   ```
   kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
   192.168.2.24
   ```

   Règle pour un ordinateur (192.168.2.25) autorisé à accéder via HTTPS à example.com (91.198.174.192) :

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
   192.168.2.25
   ```

   Règle pour l'ordinateur (192.168.2.26), qui bloque l'accès à Internet :

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
   ```

Comment ajouter une adresse IP à une zone réseau : Publique, Locale, De confiance

Le pare-feu permet de surveiller l'activité réseau pour les *zones réseau*. Une zone réseau est un groupe d'adresses IP ou de sous-réseaux regroupés sous un même type de connexion réseau. Vous pouvez utiliser une zone réseau prédéfinie pour réutiliser une règle pour plusieurs adresses IP ou sous-réseaux sans avoir à créer de règle distincte pour chaque adresse IP ou sous-réseau.

Kaspersky Endpoint Security distingue trois zones réseau :

- **Réseau public**. Le réseau n'est pas protégé par des logiciels antivirus, des pare-feu, des filtres (par exemple, le Wi-Fi dans un café). Lorsque l'utilisateur utilise un ordinateur connecté à un tel réseau, le pare-feu bloque l'accès aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur.
- **Réseau local**. Réseau pour les utilisateurs dont l'accès est limité aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).
- **Réseau de confiance**. Réseau sûr dont l'utilisation n'expose pas un ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le pare-feu autorise toute activité réseau au sein des réseaux ayant cet état.

Comment ajouter une adresse IP à une zone réseau dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.
5. Rendez-vous dans l'onglet **Réseaux disponibles**.
6. Cliquez sur **Ajouter**.

   Cette action ouvre le formulaire d'ajout d'une nouvelle connexion réseau.
7. Dans le champ **Nom**, saisissez le nom de la connexion réseau.
8. Dans le champ **Type de réseau**, sélectionnez la zone réseau à laquelle appartient la connexion réseau : **Réseau public**, **Réseau local**, **Réseau de confiance**.
9. Dans le champ **Adresse IP**, indiquez l'adresse IP ou le sous-réseau qui sera associé à la connexion réseau.
10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter une adresse IP à une zone réseau via la ligne de commande

1. Assurez-vous que la Gestion du pare-feu est activée :

   ```
   kesl-control --get-task-state 12
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 12
   ```

3. Ajoutez l'adresse à la zone réseau :

   ```
   kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
   ```

   Pour afficher la liste des règles de paquets réseau, exécutez la commande suivante :

   ```
   kesl-control -F --query
   ```

Symboles

Options de la commande

Paramètre	Description
`--add-zone`	Zone réseau prédéfinie : • `Public`. Réseau public. • `Local`. Réseau local. • `Trusted`. Réseau de confiance.
`--address`	Adresse réseau ou sous-réseau.

Exemple

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

Que sont les règles dynamiques

Kaspersky Endpoint Security permet d'ajouter ou de supprimer des *règles dynamiques* du pare-feu dont l'application a besoin pour fonctionner correctement. Par exemple :

- L'Agent d'administration ajoute des règles dynamiques qui permettent la connexion à Kaspersky Security Center.
- Le module Protection contre le chiffrement ajoute des règles dynamiques pour intercepter le trafic transmis via les protocoles de transmission et de stockage de fichiers NFS et SMB. Cela permet au module de bloquer le trafic réseau pour les appareils dont l'application interprète les actions comme un chiffrement malveillant.
- Si Kaspersky Endpoint Security est utilisé en mode Light Agent, des règles dynamiques sont automatiquement ajoutées au pare-feu qui autorisent les connexions à la SVM et au Serveur d'intégration.

Kaspersky Endpoint Security crée automatiquement des règles dynamiques qui permettent aux modules de l'application d'accéder aux ressources réseau. Les règles dynamiques ne dépendent pas de l'état du module Gestion du pare-feu (activé/désactivé) ni de l'évolution des paramètres de fonctionnement du module. La priorité d'exécution des règles dynamiques est supérieure à la priorité des règles de paquets réseau. L'application rétablit un ensemble de règles dynamiques si l'une d'elles est supprimée, par exemple à l'aide de l'utilitaire iptables. Si le processus kesl est arrêté par le serveur Watchdog, tous les liens vers les chaînes de règles créées par l'application pendant son fonctionnement (à l'exception de kesl-bypass) sont supprimés d'iptables.

Vous pouvez consulter l'ensemble des règles dynamiques à l'aide de la commande suivante :

```
kesl-control -F --query
```

L'application affiche la liste de toutes les règles pour les paquets réseau au format suivant : `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`. Les règles dynamiques sont réparties dans des chaînes distinctes : `kesl_input`, `kesl_output`, `kesl_prerouting`, `kesl_postrouting`, `kesl_forward`.

Vous ne pouvez pas gérer les paramètres des règles dynamiques.

Exemple

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

Comment créer des règles de connexion à Kaspersky Security Center

L'Agent d'administration est utilisé dans le cadre de l'interaction avec Kaspersky Security Center. Pour établir une connexion permanente entre l'Agent d'administration et Kaspersky Security Center, vous devez ajouter des règles d'autorisation pour les ports de l'Agent d'administration. Dans ce cas, même si vous configurez le pare-feu de manière incorrecte et bloquez accidentellement toutes les connexions, vous pourrez configurer le pare-feu à distance dans la console de Kaspersky Security Center.

L'ensemble des ports dépend du rôle de l'ordinateur (par exemple, point de distribution). Pour en savoir plus à propos des ports qui seront ouverts sur l'ordinateur, consultez l'aide de Kaspersky Security Center.

Ajout de règles d'autorisation pour l'Agent d'administration dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.
5. Assurez-vous que le commutateur du module est en position **Pare-feu ACTIVÉ**.
6. Cochez la case **Toujours ajouter les règles d'autorisation pour les ports de l'Agent d'administration**.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Ajout de règles d'autorisation pour l'Agent d'administration à partir de la ligne de commande

1. Assurez-vous que la Gestion du pare-feu est activée :

   ```
   kesl-control --get-task-state 12
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 12
   ```

3. Exécutez la commande:

   ```
   kesl-control --set-settings 12 OpenNagentPorts=Yes
   ```

4. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

   ```
   kesl-control --get-settings 12
   ```

Contrôles de sécurité

Contrôle des appareils

Le *Contrôle des appareils* gère l'accès des utilisateurs aux appareils installés sur l'appareil client ou connectés à celui-ci (par exemple, des disques durs, des caméras ou des modules Wi-Fi). Cela vous permet de protéger l'appareil client contre les infections lorsque des appareils externes sont connectés et d'éviter la perte ou les fuites de données.

Fonctionnement du Contrôle des appareils

Par défaut, le module Contrôle des appareils est activé et utilise les paramètres par défaut.

1. **Un utilisateur tente d'accéder à l'appareil**
2. **Le contrôle des appareils gère l'accès aux niveaux suivants :**
   - **Type d'appareil** selon la classification du module Contrôle des appareils (par exemple, imprimantes, lecteurs amovibles, lecteurs de CD/DVD). L'un des *modes d'accès* suivants peut être appliqué à chaque type d'appareil :
     - *Autoriser* pour octroyer un accès aux appareils de ce type.
     - *Bloquer* : bloque l'accès aux appareils de ce type.

- *En fonction du bus de connexion* : autoriser ou refuser l'accès aux appareils en fonction du mode d'accès du bus via lequel l'appareil est connecté.
- *Personnalisé* : autoriser ou bloquer l'accès aux appareils en fonction des règles d'accès aux appareils.
- *Lecture seule* : autoriser l'accès en lecture seule aux appareils du type sélectionné, mais l'écriture sera interdite.

- **Bus de connexion**. Le *bus de connexion* est l'interface via laquelle les appareils sont connectés à l'appareil client (par exemple, USB, FireWire). L'un des modes d'accès suivants peut être utilisé pour les bus de connexion :
  - *Autoriser* : donner accès aux appareils connectés via ce bus de connexion.
  - *Bloquer* : refuser l'accès aux appareils connectés via ce bus de connexion.

  Par exemple, l'accès à tous les appareils connectés via USB peut être refusé.

3. **Fin de l'analyse**

   Si l'appareil auquel l'utilisateur tente d'accéder n'est pas un appareil de confiance pour cet utilisateur, ou si l'utilisateur ne dispose pas de l'autorisation d'accéder à l'appareil conformément au mode d'accès, l'application bloque l'accès à l'appareil pour cet utilisateur.

   L'utilisateur peut envoyer une demande à l'administrateur de l'organisation pour signaler un blocage erroné s'il estime que c'est le cas, ou demander un accès temporaire à l'appareil.

Lorsque vous désactivez le module Contrôle des appareils, l'application déverrouille l'accès aux appareils bloqués.

Configuration du Contrôle des appareils

1. **Configurer les appareils de confiance**

   Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment. Vous pouvez accorder l'accès aux appareils de confiance à un utilisateur individuel, à un groupe d'utilisateurs ou à tous les utilisateurs de l'organisation. Par exemple, vous pouvez également autoriser l'accès à des appareils USB spécifiques ou uniquement à des clés USB, tandis que l'accès à d'autres appareils USB sera refusé.

2. **Configurer le mode d'accès**

   Vous pouvez configurer le mode d'accès pour les types d'appareils et les bus de connexion. Par défaut, le mode d'accès *Dépend du bus* est sélectionné pour tous les types d'appareils. Le mode d'accès *Autoriser* est sélectionné pour les bus de connexion. Sur la base de ces paramètres, le Contrôle des appareils donne aux utilisateurs un accès complet à tous les appareils.

3. **Configurer les règles d'accès**

   Pour les appareils de stockage (disques durs, disques amovibles, lecteurs de disquettes et lecteurs de CD/DVD), vous pouvez configurer des *règles d'accès*.

4. **Configurer le modèle de message**

   Si nécessaire, vous pouvez personnaliser le texte du modèle de message qui avertit l'utilisateur du blocage de l'accès à l'appareil ou d'une opération interdite avec l'appareil.

5. **Configurer l'accès temporaire à l'appareil**

   Si nécessaire, autorisez les utilisateurs à obtenir un accès temporaire à un appareil bloqué.

Considérations particulières et limitations

- Lors de sa première activation, le Contrôle des appareils génère un événement *Appareil autorisé* pour tous les appareils détectés dont le type d'appareil ou le type de bus est connu. Aucun événement répété n'est généré lors des exécutions ultérieures du module, sauf si les paramètres de contrôle de ces appareils ont été modifiés.
- Le contrôle des appareils ne bloque pas les disques système. Si l'application ne parvient pas à détecter automatiquement le disque système, le module Contrôle des appareils échoue avec une erreur.
- Le blocage des appareils par type d'appareil et par bus de connexion via le pilote système de l'appareil n'est pas pris en charge sur les noyaux du système d'exploitation Linux : 3.10, 5.14, 5.15, 5.17, 6.1, 6.8. Sur ces noyaux et en mode d'accès *Par règles*, seules l'ouverture de fichiers et la lecture de répertoires (c'est-à-dire l'obtention de noms de fichiers et de répertoires) sont bloquées. Sur les systèmes qui ne prennent pas en charge la technologie fanotify, le verrouillage de la lecture du répertoire n'est pas pris en charge.
- Le contrôle des appareils ignore les exclusions de points de montage. L'accès à un appareil monté sur un point de montage exclu peut être limité conformément aux paramètres configurés de contrôle des appareils.
- Si le blocage d'accès aux fichiers pendant l'analyse est désactivé dans les paramètres généraux de l'application, vous ne pouvez pas bloquer l'accès aux appareils à l'aide d'un calendrier d'accès aux appareils.

Administration de la liste des appareils de confiance à partir de la ligne de commande

La liste des appareils de confiance contient des informations sur les appareils dont l'accès est autorisé (pour des utilisateurs ou des groupes spécifiques).

La ligne de commande vous permet de consulter la liste des appareils de confiance, d'y ajouter et d'en supprimer des appareils, et d'importer une liste d'appareils de confiance à partir d'un fichier.

Afficher la liste des appareils de confiance

```
kesl-control --trusted-devices --list
```

Ajouter un appareil à la liste des appareils de confiance

```
kesl-control --trusted-devices --add <device id or mask>
```

où `<device id or mask>` est l'identifiant de l'appareil ou le masque d'identifiant de l'appareil.

Supprimer un appareil de la liste des appareils de confiance

```
kesl-control --trusted-devices --delete <device id or mask>
```

où `<device id or mask>` est l'identifiant de l'appareil ou le masque d'identifiant de l'appareil.

Importer la liste des appareils de confiance depuis un fichier

```
kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

où :

- `--merge` : fusionner les listes des appareils de confiance lors de l'importation. Si la liste actuelle et la liste importée contiennent des enregistrements pour un appareil ayant le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figurent pas dans la liste actuelle.

- `--add` : compléter la liste actuelle des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.

- `--replace` : remplacer la liste actuelle des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste importée.

- `--file <file>` est le chemin complet vers le fichier JSON à partir duquel la liste des appareils de confiance sera importée.

Configuration du mode d'accès aux appareils

Pour chaque type d'appareil (selon la classification du module Contrôle des appareils, par exemple les imprimantes, les disques amovibles, les lecteurs CD/DVD), l'un des *modes d'accès* suivants peut être appliqué :

- *Autoriser* pour octroyer un accès aux appareils de ce type.

- *Bloquer* : bloque l'accès aux appareils de ce type.

- *En fonction du bus de connexion* : autoriser ou refuser l'accès aux appareils en fonction du mode d'accès du bus via lequel l'appareil est connecté.

- *Personnalisé* : autorise ou bloque l'accès aux appareils en fonction des règles d'accès aux appareils. Une *règle d'accès à l'appareil* est un ensemble de paramètres qui définissent quels utilisateurs et à quelle heure peuvent accéder aux appareils installés ou connectés à l'appareil client. Ce mode d'accès ne peut être spécifié que pour les appareils de stockage (disques durs, disques amovibles, disquettes, lecteurs de CD/DVD).

- *Lecture seule* : autoriser l'accès en lecture seule aux appareils du type sélectionné, mais l'écriture sera interdite. Ce mode d'accès ne peut être spécifié que pour les appareils de stockage (disques durs, disques amovibles, disquettes, lecteurs de CD/DVD). Si le type d'accès à l'appareil est défini sur « Lecture seule », lorsque l'appareil de confiance est attribué à un utilisateur spécifique, l'utilisateur désigné est ignoré et l'appareil devient accessible en écriture à tous les utilisateurs.

Configuration du mode d'accès aux appareils pour les types d'appareils dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Assurez-vous que le commutateur du module est en position **Contrôle des appareils ACTIVÉ**.

6. Sous **Règles d'accès aux appareils**, dans le tableau, sélectionnez l'onglet **Appareils et réseaux Wi-Fi**.

7. Dans la colonne **Nom**, sélectionnez le type d'appareil pour lequel vous souhaitez configurer le mode d'accès.

8. Dans la liste déroulante **Accès**, sélectionnez l'un des modes d'accès suivants :

   - **Autoriser** pour octroyer l'accès aux appareils du type sélectionné.
   - **Bloquer** pour interdire l'accès aux appareils du type sélectionné.
   - **Dépend du bus** (valeur par défaut) pour autoriser ou interdire l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion.
   - **Personnalisé** : autorise ou bloque l'accès aux appareils en fonction de la règle d'accès et de la planification. Cette option est disponible uniquement pour les appareils de stockage (disques durs, disques amovibles, lecteurs de disquettes, lecteurs CD/DVD).
   - **Lecture seule** : autoriser l'accès en lecture seule aux appareils du type sélectionné. Cette option est disponible uniquement pour les appareils de stockage (disques durs, disques amovibles, lecteurs de disquettes, lecteurs CD/DVD).

9. Dans le tableau ci-dessous, cliquez sur le bouton **Ajouter**.

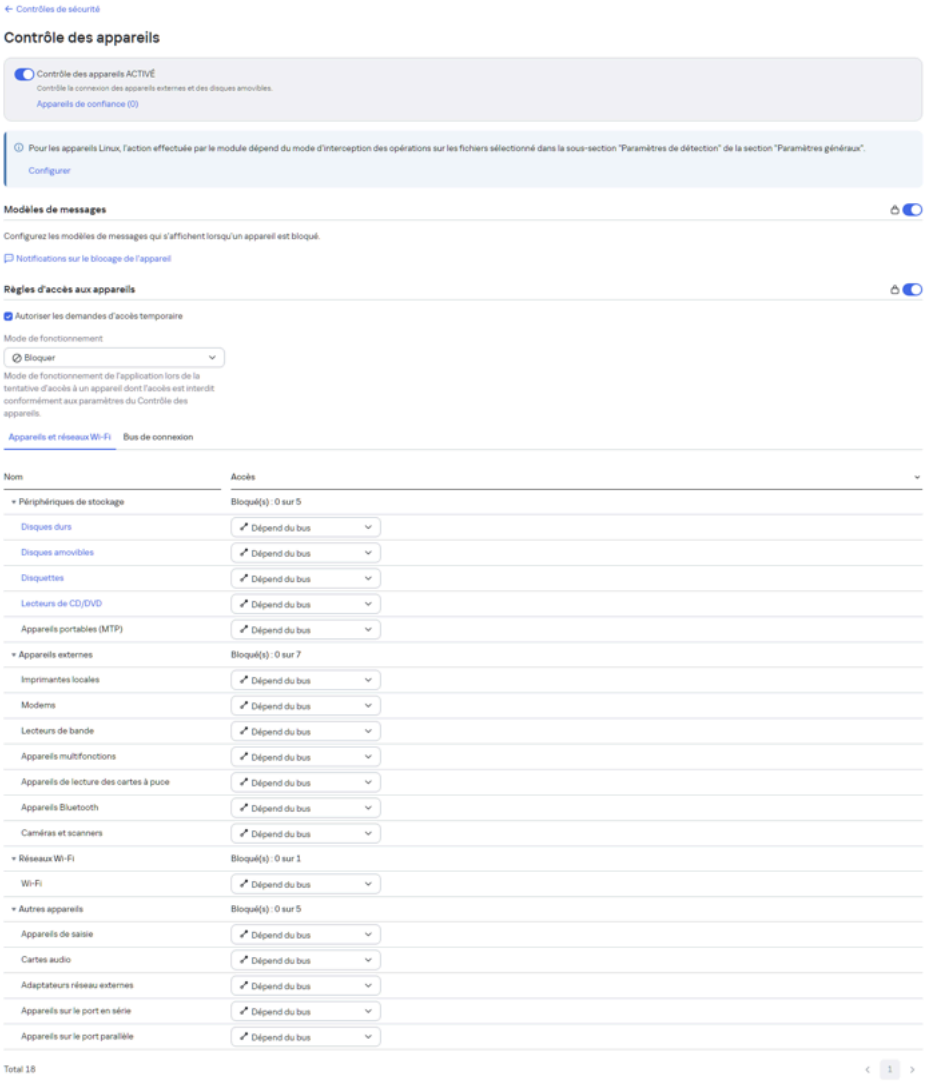
   Une fenêtre s'ouvre pour ajouter une nouvelle règle d'accès.

10. Dans le champ **Priorité**, définissez la priorité de la règle d'accès.

11. Sélectionnez les utilisateurs ou le groupe d'utilisateurs auxquels la règle d'accès s'appliquera. Par défaut, la règle s'applique à tous les utilisateurs.

12. Si nécessaire, définissez une planification de l'accès. Par défaut, la règle est toujours appliquée.

13. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Contrôle des appareils

Configuration du mode d'accès aux appareils pour les types d'appareils à partir de la ligne de commande

1. Assurez-vous que le module Contrôle des appareils est en cours d'exécution :

   ```
   kesl-control --get-task-list
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 15
   ```

3. Sélectionnez le mode de fonctionnement lors d'une tentative d'accès à un appareil dont l'accès est restreint conformément aux règles du Contrôle des appareils :

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

4. Spécifiez le mode d'accès pour l'un des types d'appareils : `HardDrive`, `RemovableDrive`, `FloppyDrive`, `OpticalDrive`, `SerialPortDevice`, `ParallelPortDevice`, `Printer`, `Modem`, `TapeDrive`, `MultifuncDevice`, `SmartCardReader`, `WiFiAdapter`, `NetworkAdapter`, `PortableDevice`, `PortableDevice`, `BluetoothDevice`, `ImagingDevice`, `SoundAdapter`, `InputDevice`

```
kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
```

5. Pour afficher les paramètres du Contrôle des appareils, exécutez la commande suivante :

```
kesl-control --get-settings 15
```

Configuration du mode d'accès au bus de connexion dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des appareils ACTIVÉ**.
6. Sous **Règles d'accès aux appareils**, dans le tableau, sélectionnez l'onglet **Bus de connexion**.
7. Dans la colonne **Nom**, sélectionnez le bus pour lequel vous souhaitez configurer le mode d'accès.
8. Dans la liste déroulante **Accès**, sélectionnez l'un des modes d'accès suivants :
   - **Autoriser** : donner accès aux appareils connectés via ce bus de connexion.
   - **Bloquer** : refuser l'accès aux appareils connectés via ce bus de connexion.
9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration du mode d'accès au bus de connexion à partir de la ligne de commande

1. Assurez-vous que le module Contrôle des appareils est en cours d'exécution :

```
kesl-control --get-task-list
```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

```
kesl-control --start-task 15
```

3. Sélectionnez le mode de fonctionnement lors d'une tentative d'accès à un appareil dont l'accès est restreint conformément aux règles du Contrôle des appareils :

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Spécifiez le mode d'accès pour les bus de connexion :

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. Pour afficher les paramètres du Contrôle des appareils, exécutez la commande suivante :

```
kesl-control --get-settings 15
```

Comment configurer les règles d'accès aux appareils

Pour les appareils de stockage (disques durs, disques amovibles, lecteurs de disquettes et lecteurs de CD/DVD), vous pouvez configurer des règles d'accès. *Une règle d'accès à l'appareil* est un ensemble de paramètres qui définissent quels utilisateurs peuvent accéder aux appareils installés sur l'appareil client ou connectés à celui-ci, et à quel moment. Ce mode d'accès ne peut être spécifié que pour les appareils de stockage (disques durs, disques amovibles, disquettes, lecteurs de CD/DVD). Lorsque vous connectez un appareil dont l'accès est interdit, l'application refuse aux utilisateurs spécifiés dans la règle l'accès à cet appareil et affiche une notification. Lors d'une tentative de lecture et d'écriture sur cet appareil, l'application refuse la lecture/écriture aux utilisateurs spécifiés dans la règle sans afficher de notification. Si, lorsque vous tentez d'effectuer une opération sur un appareil pour lequel le mode d'accès *En fonction des règles* est défini, aucune règle n'est active au moment de l'accès, l'opération avec l'appareil sera interdite.

Comment configurer une règle d'accès aux appareils dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des appareils ACTIVÉ**.
6. Sous **Règles d'accès aux appareils**, dans le tableau, sélectionnez l'onglet **Appareils et réseaux Wi-Fi**.
7. Dans la colonne **Nom**, sélectionnez le type d'appareil de stockage pour lequel vous souhaitez ajouter une règle d'accès (disques durs, disques amovibles, lecteurs de disquettes, lecteurs de CD / DVD).
8. Dans la fenêtre qui s'ouvre, sous **Règles d'accès aux appareils**, sélectionnez **Personnalisé**.
9. Dans le tableau ci-dessous, cliquez sur le bouton **Ajouter**.

   Une fenêtre s'ouvre pour ajouter une nouvelle règle d'accès.
10. Dans le champ **Priorité**, définissez la priorité de la règle d'accès.

11. Sélectionnez les utilisateurs ou le groupe d'utilisateurs auxquels la règle d'accès s'appliquera. Par défaut, la règle s'applique à tous les utilisateurs.

12. Si nécessaire, définissez une planification de l'accès. Par défaut, la règle est toujours appliquée.

13. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer une règle d'accès aux appareils en ligne de commande

1. Assurez-vous que le module Contrôle des appareils est en cours d'exécution :

   ```
   kesl-control --get-task-list
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 15
   ```

3. Pour afficher les paramètres du Contrôle des appareils, exécutez la commande suivante :

   ```
   kesl-control --get-settings 15
   ```

4. Sélectionnez le mode de fonctionnement lors d'une tentative d'accès à un appareil dont l'accès est restreint conformément aux règles du Contrôle des appareils :

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

5. Ajoutez une nouvelle règle d'accès pour l'un des types d'appareils suivants : `HardDrivePrincipals.item_#.AccessRules.item_#`, `RemovableDrivePrincipals.item_#.AccessRules.item_#`, `FloppyDrivePrincipals.item_#.AccessRules.item_#` ou `OpticalDrivePrincipals.item_#.AccessRules.item_#`.

   - Activez la règle et spécifiez la planification par défaut :

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     Exemple

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Définissez l'action du Contrôle des appareils lorsque la règle est déclenchée :

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     Exemple

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Si nécessaire, spécifiez les utilisateurs auxquels la règle s'appliquera :

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     Exemple

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - Si nécessaire, modifiez la planification de la règle :

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     Exemple

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

Configuration du modèle de message du Contrôle des appareils

Lorsqu'un utilisateur tente d'accéder à un appareil verrouillé, l'application affiche un message indiquant que l'accès à l'appareil est refusé ou que les opérations sur l'appareil sont interdites.

Un modèle est fourni pour les messages de refus d'accès, décrivant les raisons du blocage. Il existe des variables spéciales pour le texte du modèle de message (par exemple, %USER_NAME%). Les variables vous permettent d'utiliser un seul modèle de message pour différents appareils. Lors de la génération d'un message, l'application insère dans celui-ci les valeurs des variables correspondant à un appareil, un utilisateur et un événement spécifiques.

Vous pouvez modifier le contenu du modèle de message.

Comment modifier le modèle de message dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.
5. Sous **Modèles de messages**, cliquez sur le lien **Notifications sur le blocage de l'appareil**.

   La fenêtre de configuration du modèle de message s'ouvre.
6. Configurez le modèle de message du Contrôle des appareils dans l'onglet **Message à l'utilisateur**.
7. Vous pouvez ajouter des variables et des liens au texte du message adressé à l'utilisateur à l'aide des boutons **Ajouter une variable** et **Ajouter un lien**. Pour ajouter une variable au texte du modèle, placez le curseur à l'endroit souhaité dans le texte, cliquez sur le bouton **Ajouter une variable** et sélectionnez la variable souhaitée dans la liste déroulante. Pour ajouter un lien au texte du modèle, placez le curseur à l'endroit souhaité dans le texte et cliquez sur le bouton **Ajouter un lien**.

   Si vous souhaitez restaurer le texte du modèle de message, cliquez sur le bouton **Restaurer par défaut**.
8. Cliquez sur le bouton **OK**.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Comment modifier un modèle de message dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.
4. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de sécurité** → **Contrôle des appareils**.
5. Dans la section **Modèles** de messages, cliquez sur le bouton **Configurer**.
6. Dans la fenêtre **Modèles de messages** qui s'ouvre, configurez le modèle de message du Contrôle des appareils sous l'onglet **Message sur le blocage**.

Vous pouvez ajouter des variables et des liens au texte d'un message destiné à un utilisateur à l'aide des boutons **Variable** et **Lien**. Pour ajouter une variable au texte du modèle, placez le curseur à l'endroit souhaité dans le texte, cliquez sur le bouton **Variable** et sélectionnez la variable souhaitée dans la liste déroulante. Pour ajouter un lien au texte du modèle, placez le curseur à l'endroit souhaité dans le texte et cliquez sur le bouton **Lien**.

Vous pouvez aussi restaurer le texte du modèle de message en cliquant sur le bouton **Par défaut**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Appliquer**.

Autorisation d'accès temporaire à l'appareil

Lors de la configuration du Contrôle des appareils, l'administrateur peut bloquer accidentellement l'accès à un appareil nécessaire au travail d'un utilisateur. Si l'utilisateur pense que l'accès à un appareil ou à son contenu a été bloqué par erreur, il peut demander un accès temporaire à l'appareil bloqué auprès de l'administrateur réseau local de l'organisation.

Il est possible de demander un accès temporaire si l'administrateur a autorisé l'utilisateur à en faire la demande. L'administrateur peut configurer cette autorisation dans les propriétés de la stratégie, soit dans Web Console, soit dans la Console d'administration, soit encore dans les paramètres de la tâche Contrôle des appareils.

La procédure d'autorisation d'accès à un appareil bloqué se déroule comme suit :

1. L'utilisateur crée un *fichier de demande* et le soumet à l'administrateur, par exemple par email ou tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage). L'utilisateur peut demander un accès temporaire à un appareil bloqué dans l'interface graphique de l'application ou via la ligne de commande.

2. L'administrateur crée une *clé d'accès* à partir du fichier de requête et la transmet à l'utilisateur, par exemple, par message ou tout autre moyen disponible. L'accès à un appareil bloqué est accordé dans Web Console.

3. L'utilisateur télécharge la clé d'accès et obtient un accès temporaire à l'appareil verrouillé. L'utilisateur peut télécharger la clé d'accès via l'interface utilisateur graphique ou la ligne de commande de l'application.

L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.1 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.

Comment créer une clé d'accès pour l'appareil bloqué dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration qui contient l'appareil dont vous avez besoin et cochez la case en regard de son nom.

3. Au-dessus de la liste des appareils administrés, cliquez sur le bouton **Accorder l'accès à l'appareil en mode hors-ligne**. Si le bouton n'apparaît pas au-dessus de la liste des appareils, cliquez sur le bouton représentant des points de suspension et sélectionnez l'option **Partager cet appareil en mode hors-ligne** dans le menu.

4. Dans la fenêtre **Paramètres de l'application** qui s'ouvre, dans la section **Contrôle des appareils**, cliquez sur le bouton **Parcourir** et chargez le fichier de requête reçu de l'utilisateur.

   Les informations relatives à l'appareil bloqué auquel l'utilisateur a demandé l'accès seront affichées.

5. Si nécessaire, modifiez la valeur en heures dans le champ **Durée d'accès**.

   Par défaut, le champ **Durée d'accès** est défini sur la valeur spécifiée par l'utilisateur lors de la génération du fichier de requête d'accès.

6. Si nécessaire, modifiez la valeur du champ **Spécifiez la période pendant laquelle la clé d'accès peut être utilisée sur l'appareil client**.

   Le champ indique la période pendant laquelle l'utilisateur peut télécharger la clé d'accès.

7. Cliquez sur le bouton **Créer une clé**.

8. Enregistrez le fichier contenant la clé d'accès avec l'extension *.acode.

Comment demander et obtenir un accès temporaire via la ligne de commande

Si l'utilisateur estime que l'accès à l'appareil a été bloqué ou qu'une opération avec le contenu de l'appareil a été interdite par erreur, il peut demander un accès temporaire à l'appareil bloqué auprès de l'administrateur du réseau local de l'organisation à l'aide de la commande d'administration du Contrôle des appareils suivante :

```
Demander un accès temporaire à un appareil bloqué

kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access
duration> --path <path to the access request file>
```

où :

`--device-id <device identifier>` est l'identifiant de l'appareil verrouillé auquel vous souhaitez accéder.

`--access-duration <access duration>` est la période pendant laquelle vous souhaitez accéder à l'appareil (en heures). Valeurs possibles : 1 à 100.

`--path <path to the access request file>` est le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.

À la suite de l'exécution de la commande, un fichier de demande d'accès sera créé, qui devra être envoyé à l'administrateur, par exemple par courrier électronique ou par tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage).

Après avoir reçu la clé d'accès de l'administrateur, vous devez saisir la clé d'accès pour obtenir un accès temporaire à l'appareil.

```
Charger une clé d'accès pour un appareil bloqué

kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

où :

`--path <path to the file with the access key>` est le chemin d'accès au fichier contenant la clé d'accès à l'appareil (fichier avec l'extension .acode).

La commande affiche des informations sur l'accès à l'appareil et sur la période pendant laquelle l'accès à cet appareil est accordé.

Comment demander et obtenir un accès temporaire dans l'interface graphique

Lors de la connexion d'un appareil bloqué par le Contrôle des appareils, une fenêtre s'ouvre avec un message vous informant que l'accès à l'appareil est bloqué.

Vous pouvez demander un accès temporaire à un appareil bloqué auprès de l'administrateur réseau local de votre organisation en utilisant l'interface graphique de la manière suivante :

- depuis la fenêtre affichant un message concernant le blocage de l'accès à l'appareil en cliquant sur le bouton **OK**.
- depuis la fenêtre principale de l'interface graphique de l'application.

Pour demander un accès temporaire à un appareil verrouillé :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Accès temporaire**.

   La fenêtre **Accès temporaire** s'ouvrira.

   Vous pouvez également ouvrir la fenêtre **Accès temporaire** à partir de la fenêtre affichant le message concernant le blocage de l'accès à l'appareil en cliquant sur le bouton **OK**.
3. Dans la section **Demander l'accès à un appareil bloqué**, dans la liste des appareils connectés, sélectionnez l'appareil auquel vous souhaitez accéder.
4. Dans le champ **Durée d'accès à l'appareil en heures**, spécifiez la période pendant laquelle vous souhaitez accéder à l'appareil (en heures).
5. Cliquez sur le bouton **Générer le fichier de demande**.
6. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.
7. Transmettez le fichier de demande d'accès à l'administrateur, par exemple par email ou tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage).

Une fois que vous aurez reçu la clé d'accès de l'administrateur, vous pourrez la télécharger pour obtenir un accès temporaire à l'appareil verrouillé.

Pour obtenir un accès temporaire à un appareil verrouillé :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Accès temporaire**.

   La fenêtre **Accès temporaire** s'ouvrira.
3. Dans la section **Accès à l'appareil**, cliquez sur le bouton **Télécharger la clé d'accès**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la clé d'accès à l'appareil (fichier clé avec l'extension .acode) reçue de l'administrateur du réseau local de l'organisation.
5. Une fenêtre s'ouvre affichant des informations sur l'appareil auquel l'accès a été accordé, ainsi que la durée de cet accès.
6. Cliquez sur le bouton **OK**.

Contrôle Internet

Le Contrôle Internet contrôle l'accès des utilisateurs aux ressources Internet. Cela vous permet de réduire la consommation de trafic et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur tente d'ouvrir un site dont l'accès est restreint par le Contrôle Internet, l'application Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement.

Le Contrôle Internet permet de restreindre l'accès aux ressources Internet en fonction de la catégorie de contenu et du type de données, ainsi que de bloquer l'accès à des sites Internet particuliers. Vous pouvez restreindre l'accès des utilisateurs, par exemple, à la catégorie du contenu « Réseaux sociaux » ou à d'autres catégories. L'application détermine le type de données d'après le format du fichier, et non d'après l'extension.

Fonctionnement du Contrôle Internet

1. **L'application vérifie les requêtes adressées aux ressources Internet**

   Le Contrôle Internet détermine la catégorie de contenu et le type de données d'un site Internet à l'aide des technologies suivantes :

   - Bases antivirus.
   - Services cloud de Kaspersky Security Network.
   - La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

2. **L'application applique les règles**

   L'application applique les règles du Contrôle Internet par ordre de priorité. Plus le numéro de priorité est bas, plus la priorité de la règle est élevée. Si plusieurs règles s'appliquent à un site Internet, le Contrôle Internet applique la règle dont la priorité est la plus élevée.

   Par exemple, une application peut définir un portail d'entreprise comme un réseau social. Pour limiter l'accès aux réseaux sociaux et octroyer un accès au portail de l'entreprise, créez deux règles : une règle d'interdiction pour la catégorie de sites *Réseaux sociaux* et une règle d'autorisation pour le portail de l'entreprise. La règle d'accès au portail Web d'entreprise doit avoir une priorité plus élevée que la règle d'accès aux réseaux sociaux.

3. **Fin de l'analyse**

   Si une règle bloque l'accès à une ressource Internet, l'application affiche un message de blocage dans le navigateur. La ressource devient indisponible.

   L'utilisateur peut envoyer une demande à l'administrateur de l'organisation concernant le blocage erroné s'il estime que la page Internet a été bloquée par erreur.

Configuration du Contrôle Internet

1. **Configurer les règles du Contrôle Internet**

   Le Contrôle Internet gère l'accès des utilisateurs aux sites Internet à l'aide de *règles d'accès*. Ces règles permettent de restreindre l'accès aux sites Internet pour des utilisateurs particuliers, ainsi que de configurer un calendrier d'accès.

   Par exemple, vous pouvez restreindre l'accès aux sites Internet de la catégorie *Communication via Internet* pour tous les utilisateurs de l'organisation, à l'exception du service informatique.

2. **Configurer les modèles de messages**

   Selon l'action de la règle d'accès, le Contrôle Internet affiche à l'utilisateur un message concernant la visite d'un site Internet indésirable ou un message de blocage. Lorsqu'un site Internet est bloqué, l'utilisateur peut envoyer un message à l'administrateur du réseau local concernant le blocage erroné.

   Des modèles sont prévus pour ces messages.

   > Les modèles ne peuvent pas être modifiés sur la ligne de commande.

3. **Activer le Contrôle Internet**

   Par défaut, le Contrôle Internet est désactivé. Activez le module dans Web Console ou dans la Console d'administration à l'aide du commutateur, ou sur la ligne de commande à l'aide de la commande suivante :

   ```
   kesl-control --start-task 26
   ```

Considérations particulières et limitations

- L'application n'analyse pas les fichiers dans les archives. Par exemple, si des fichiers image sont archivés, l'application détectera le type de données comme « Archives » plutôt que « Fichiers graphiques ».
- Kaspersky Endpoint Security contrôle uniquement le trafic HTTP et HTTPS.
- Lorsque la Protection contre les menaces Internet et le Contrôle Internet fonctionnent simultanément, les paramètres de la Protection contre les menaces Internet sont appliqués à la ressource Internet. Cela signifie qu'un site Internet malveillant ou de phishing est bloqué même si les règles du Contrôle Internet en autorisent l'accès.

Comment créer une règle d'accès aux ressources Internet

Une *règle d'accès aux ressources Internet* est un ensemble de filtres et d'actions que Kaspersky Endpoint Security applique lorsque les utilisateurs visitent des ressources Internet. Les règles d'accès peuvent inclure une planification de règles.

Les règles restreignent l'accès aux ressources Internet selon les filtres suivants :

- **Catégories de contenu**. Le Contrôle Internet classe les ressources Internet par contenu et par type de données. Cela permet de restreindre l'accès des utilisateurs aux sites Internet présentant une catégorie de contenu spécifique (par exemple, *Systèmes de paiement*) et/ou un type de données spécifique (par exemple, *Fichiers exécutables*).

- **Sites Internet individuels**. Le Contrôle Internet permet de restreindre l'accès des utilisateurs à des adresses individuelles ou à des groupes d'adresses de ressources Internet.

  Les domaines des adresses Internet ne sont pas sensibles à la casse. Si une règle contient une adresse Internet telle que `examPLE.com`, le Contrôle Internet restreint l'accès à `example.com`.

  Si un filtre par catégorie de contenu et un filtre par sites Internet individuels sont configurés simultanément dans une règle d'accès, le Contrôle Internet ne restreint pas l'accès à tous les sites Internet de la catégorie de contenu indiquée, mais uniquement aux adresses Internet indiquées.

- **Filtrer par noms d'utilisateurs et groupes d'utilisateurs**. Le Contrôle Internet permet de restreindre l'accès aux ressources Internet pour des utilisateurs individuels ou des groupes d'utilisateurs. Par exemple, vous pouvez restreindre l'accès aux sites Internet de réseaux sociaux à tous les utilisateurs de l'organisation, à l'exception du service informatique.

- **Planification de l'application de la règle**. La planification de la règle détermine l'heure à laquelle l'application contrôle l'accès aux ressources Web spécifiées dans la règle. Par exemple, vous pouvez restreindre l'accès aux sites Internet indésirables uniquement pendant les heures de travail.

Si aucune règle de refus n'a été créée, le trafic HTTPS n'est pas déchiffré.

Comment créer une règle d'accès dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.
5. Assurez-vous que le commutateur du module est en position **Contrôle Internet ACTIVÉ**.
6. Sous **Liste des règles**, sélectionnez l'action par défaut du Contrôle Internet :

   - **Autoriser tout ce qui ne figure pas dans la liste des règles**
   - **Bloquer tout ce qui ne figure pas dans la liste des règles**
7. Cliquez sur **Ajouter**.

   Cette action ouvre le formulaire permettant d'ajouter une nouvelle règle d'accès.
8. Dans le champ **Nom de la règle**, saisissez le nom de la règle. Le nom de la règle doit être unique.
9. Dans le champ **Priorité**, définissez la priorité de la règle d'accès.

10. Sélectionnez l'action que le Contrôle Internet doit appliquer aux ressources Internet lorsque la règle se déclenche :

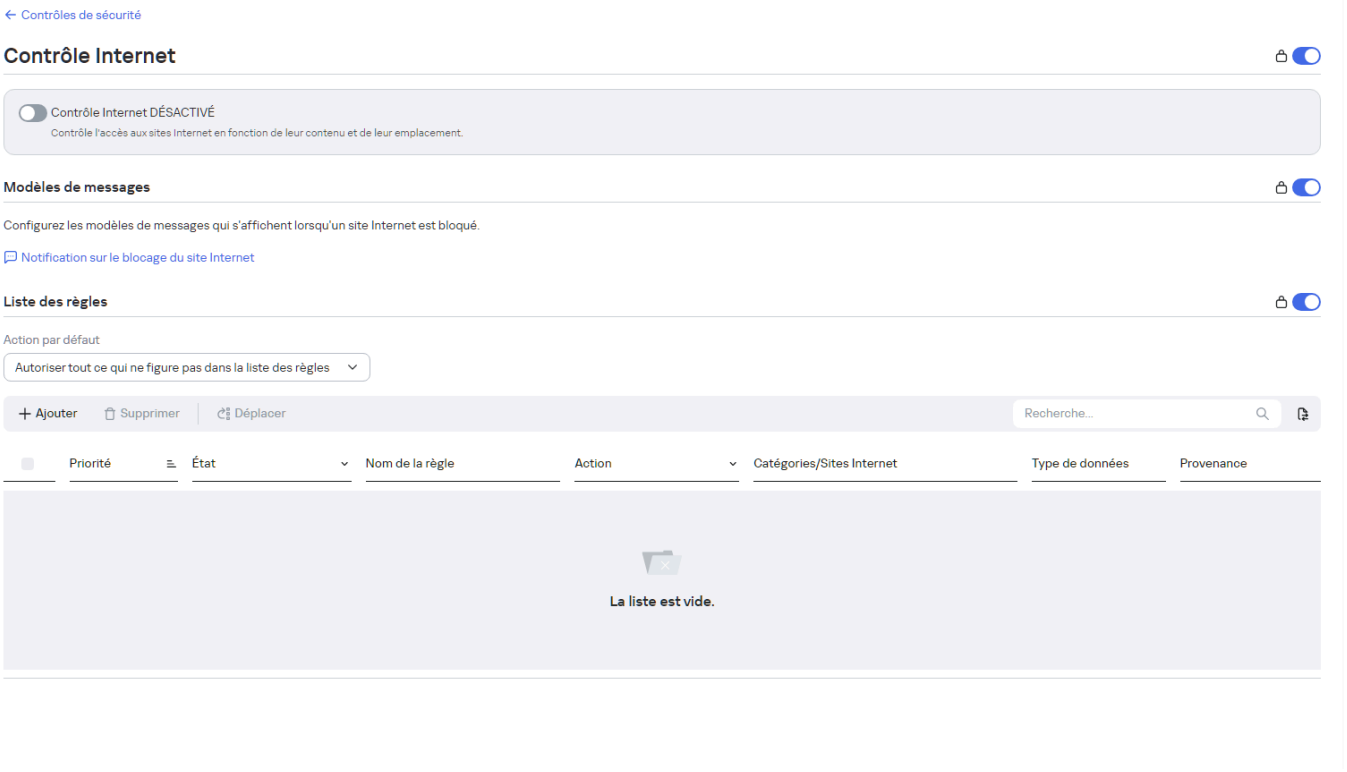
    - **Autoriser**. Le Contrôle Internet permet à l'utilisateur d'accéder à une ressource Web.
    - **Interdire**. Le Contrôle Internet refuse à l'utilisateur l'accès à la ressource Web et affiche un message concernant le refus d'accès. En cliquant sur les liens du message de blocage, l'utilisateur peut envoyer un message à l'administrateur du réseau local pour signaler une erreur de blocage.
    - **Informer**. Le Contrôle Internet affiche un avertissement concernant la consultation d'une ressource Internet indésirable. Si l'utilisateur estime que l'avertissement est incorrect, le lien figurant dans l'avertissement lui permet d'accéder à une page Internet ou d'envoyer une demande à l'administrateur du réseau local de l'organisation.

11. Sélectionnez un filtre de règle d'accès :

    - **Catégories de contenu**. Spécifiez les catégories de contenu que la règle d'accès doit contrôler. Vous pouvez sélectionner plusieurs catégories.
    - **Sites Internet individuels**. Spécifiez une adresse de site Internet ou un groupe de sites Internet.

    > Dans Web Console, vous ne pouvez pas configurer simultanément un filtre par catégorie de contenu et un filtre par sites Internet individuels.

12. Si nécessaire, indiquez les types de données que l'application doit filtrer.
13. Sélectionnez les utilisateurs ou le groupe d'utilisateurs auxquels la règle d'accès s'appliquera. Par défaut, la règle s'applique à tous les utilisateurs.
14. Si nécessaire, définissez une planification de l'accès. Par défaut, la règle est toujours appliquée.
15. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Comment créer une règle d'accès en ligne de commande

1. Assurez-vous que le module Contrôle Internet est activé :

   ```
   kesl-control --get-settings 26
   ```

   Le module doit avoir l'état **Démarré**.

2. Si le module est désactivé, exécutez la commande suivante :

   ```
   kesl-control --start-task 26
   ```

3. sélectionnez l'action par défaut du Contrôle Internet :

   ```
   kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
   ```

4. Ajoutez une nouvelle règle d'accès avec l'ID `#` :

   a. Activez la règle :

   ```
   kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
   ```

   b. Saisissez le nom de la règle :

   ```
   kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
   ```

   c. Spécifiez l'action que le Contrôle Internet doit appliquer aux ressources Internet lorsque la règle se déclenche :

   ```
   kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
   ```

   d. Si vous devez filtrer les ressources Internet par catégorie de contenu :

   ```
   kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
   kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
   [Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
   ```

   e. Si vous devez filtrer des ressources Internet individuelles :

   ```
   kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
   kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
   ```

   f. Si nécessaire, indiquez les utilisateurs auxquels la règle s'appliquera :

   ```
   kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
   kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
   ```

g. Si nécessaire, définissez une planification pour la règle :

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. Pour afficher la liste des règles du Contrôle Internet, exécutez la commande suivante :

```
kesl-control --get-settings 26
```

Symboles

Options de la commande

Paramètre	Description
`WebControlDefaultAction`	Action que le Contrôle Internet applique aux ressources Web qui ne sont indiquées dans aucune règle d'accès.
`Enabled=Yes`	Activer la règle d'accès dont l'ID est `#`.
`Name`	Nom de la règle. Le nom de la règle doit être unique.
`WebControlAction`	Action que le Contrôle Internet applique aux ressources Web lorsque la règle est déclenchée : `Allow` (valeur par défaut) : autoriser l'accès à la ressource Web. `Block` : interdire l'accès à une ressource Web. `Notify` – afficher un avertissement concernant la visite d'une ressource Web indésirable. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.
`UseCategories`	Utilisation de filtres par catégories de contenu et par catégories de types de données dans la règle : `None` (valeur par défaut) : ne pas utiliser le filtre de contenu des ressources Web. `ContentOnly` : utiliser un filtre par catégories de contenu dans la règle. `FormatOnly` : utiliser un filtre pour les catégories de types de données dans la règle. `ContentAndFormat` : utiliser un filtre dans la règle par catégories de contenu et catégories de types de données.
`ContentCategories.item_#.ContentCategory`	Catégorie de contenu.
`FormatCategories.item_#.FormatCategory`	Catégorie de types de données : `Video` – Fichiers vidéo `Audio` – Fichiers audio `OfficeDocument` : fichiers des applications Office `Executable` : fichiers exécutables `Archives` : archives `Images` : fichiers graphiques `Scripts` : scripts
`UseUrls=Yes`	Utilisation de sites Web individuels dans une règle de filtrage.
`Urls.item_#`	L'adresse de la ressource Web, dont l'accès est réglementé par la règle. Vous pouvez utiliser des masques pour spécifier l'adresse d'une ressource Web.
`UsePrincipals=Yes`	Utilisation d'un filtre pour les utilisateurs soumis à une règle d'accès aux ressources Web.
`Principals.item_#.Name`	Utilisateur ou groupe d'utilisateurs soumis à la règle d'accès aux ressources Web : `<user name>` est le nom de l'utilisateur auquel la règle s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle s'applique.
`Schedules.item_#.Id`	ID de la planification.
`Schedules.item_#.Name`	Spécifie un nom de planification.

Paramètre	Description
`Schedules.item_#.DaysHours`	Spécifie les intervalles de temps d'une planification : `<day of week>` est le jour de la semaine. Vous pouvez utiliser les noms complets des jours de la semaine ou leurs abréviations (par exemple, pour lundi, vous pouvez spécifier `Mo`, `Mon` ou `Monday`). Pour les jours de la semaine, vous pouvez spécifier des intervalles ou des jours spécifiques. La semaine commence le dimanche. `<hour>` – Heures [0:24]. Pour les heures, vous ne pouvez spécifier que des intervalles.

Comment modifier les modèles de messages du Contrôle Internet

En fonction de l'action spécifiée dans la règle d'accès, lorsqu'un utilisateur tente d'accéder à des ressources Internet, le Contrôle Internet affiche un message à l'utilisateur (en remplaçant la réponse du serveur HTTP par une page HTML contenant un message) :

- **Message d'alerte.** Le message affiché à l'utilisateur lorsqu'il tente de consulter une ressource indésirable. L'application affiche ce message si l'action **Informer** est sélectionnée pour la règle.

  Si l'utilisateur estime que l'avertissement est incorrect, le lien figurant dans l'avertissement lui permet d'accéder à une page Internet ou d'envoyer une demande à l'administrateur du réseau local de l'organisation.

- **Message relatif à une ressource Internet bloquée** Message affiché à l'utilisateur lorsqu'une ressource Internet indésirable est bloquée. L'application affiche ce message si l'action **Interdire** est sélectionnée pour la règle.

  Si l'utilisateur estime qu'une ressource Internet a été bloquée par erreur, le lien contenu dans le message de blocage de la ressource Internet lui permet d'envoyer une requête à l'administrateur du réseau local de l'organisation.

Des modèles sont fournis pour les messages d'avertissement, les messages relatifs au blocage d'une ressource Internet et les requêtes adressées à l'administrateur du réseau local de l'organisation. Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.

Les modèles ne peuvent pas être modifiés sur la ligne de commande.

Comment modifier le modèle de message dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.
5. Sous **Modèles de messages**, cliquez sur le lien **Notification sur le blocage du site Internet**.

   La fenêtre contenant les modèles de messages s'ouvre.

6. Configurez les modèles de messages du Contrôle Internet :

   - **Avertissement**. Le modèle de l'avertissement affiché à l'utilisateur lorsqu'il tente de consulter une ressource indésirable.

   - **Notification sur le blocage**. Le modèle du message affiché lors du blocage d'une page Web ou d'un site Internet indésirable.

   - **Message pour l'administrateur**. Modèle d'un message adressé à l'administrateur. Utilisé si l'utilisateur estime que la page Web a été bloquée par erreur. Une fois que l'utilisateur a demandé l'accès, l'application envoie un événement *Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet* à Kaspersky Security Center. La description de l'événement contient un message destiné à l'administrateur avec des variables substituées. Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'y a pas de connexion avec le Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Si vous souhaitez restaurer le texte du modèle de message, cliquez sur le bouton **Réinitialiser le texte par défaut**.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment modifier un modèle de message dans la Console d'administration

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de sécurité → Contrôle Internet**.

5. Dans la section **Modèles** de messages, cliquez sur le bouton **Configurer**.

6. Dans la fenêtre **Modèles de messages** qui s'ouvre, configurez les modèles de messages du Contrôle Internet sous les onglets suivants :

   - **Avertissement**. Le champ de saisie contient un modèle de message qui apparaît lorsqu'une règle est déclenchée, avertissant d'une tentative d'accès à une ressource Web non recommandée.

   - **Message sur le blocage**. Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui bloque l'accès au site Internet est appliquée.

   - **Plainte auprès de l'administrateur**. Le champ de saisie contient un modèle de message de réclamation à envoyer à l'administrateur du réseau local de l'organisation si, de l'avis de l'utilisateur, l'accès à la ressource Web a été bloqué par erreur. Lorsqu'un utilisateur demande l'autorisation d'accéder, l'application Kaspersky Endpoint Security envoie à Kaspersky Security Center un événement *Message à l'administrateur concernant l'accès refusé à une page Web*. La description de l'événement contient un message destiné à l'administrateur avec des variables substituées. Vous pouvez afficher ces événements dans la Console d'administration de Kaspersky Security Center à l'aide de la sélection prédéfinie **Demandes des utilisateurs**. Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'y a pas de connexion avec le Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Sous les onglets **Avertissement** et **Message sur le blocage**, vous pouvez ajouter des variables et des liens vers des textes de message destinés à l'utilisateur à l'aide des boutons **Variable** et **Lien**.

Vous pouvez restaurer le texte du modèle de message en cliquant sur le bouton **Par défaut**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Appliquer**.

Règles de formation des masques d'adresses de ressources Web

L'utilisation d'*un masque d'adresse de ressource Web* (ci-après également appelé « masque d'adresse ») peut être pratique dans les cas où, lors du processus de création d'une règle d'accès aux ressources Web, vous devez saisir de nombreuses adresses de ressources Web similaires. Un masque d'adresse bien formé peut remplacer de nombreuses adresses de ressources Web.

Lors de la génération d'un masque d'adresse, les règles suivantes doivent être utilisées :

1. Le caractère `*` remplace toute séquence de zéro ou plusieurs caractères.

   Par exemple, lorsque vous saisissez le masque d'adresse `*abc*`, la règle d'accès aux ressources Web est appliquée à toutes les adresses contenant la séquence `abc`. Exemple : `http://www.example.com/page_0-9abcdef.html`.

2. Séquence de caractères `*.` vous permet de sélectionner tous les domaines d'adresse : *masque de domaine*. Masque de domaine `*.` est traité comme n'importe quel nom de domaine, nom de sous-domaine ou chaîne vide.

   Exemple : les adresses suivantes sont soumises au masque `*.example.com` :

   - `http://pictures.example.com` – le masque de domaine `*.` correspond à `pictures.`.
   - `http://user.pictures.example.com` – le masque de domaine `*.` correspond à `pictures.` et `user.`.
   - `http://example.com` : masque de domaine `*.` est traité comme une chaîne vide.

3. La séquence de caractères `www.` au début du masque d'adresse est interprété comme la séquence `*.`.

   Exemple : le masque d'adresse `www.example.com` est interprété comme `*.example.com`. Le masque couvre les adresses `www2.example.com` et `www.pictures.example.com`.

4. Si le masque d'adresse ne commence pas par le caractère `*`, alors le contenu du masque d'adresse est équivalent au même contenu préfixé par `*.`.

5. Si un masque d'adresse se termine par un caractère autre que `/` ou `*`, alors le contenu du masque d'adresse est équivalent au même contenu avec un suffixe `/*`.

   Exemple : le masque d'adresse `http://www.example.com` comprend des adresses de la forme `http://www.example.com/abc`, où `a`, `b`, `c` sont des caractères quelconques.

6. Si un masque d'adresse se termine par un caractère `/`, alors le contenu du masque d'adresse est équivalent au même contenu avec le suffixe `/*`.

7. La séquence des caractères `/*` à la fin du masque d'adresse est traitée comme `/*` ou comme la ligne vide.

8. La vérification des adresses des ressources Web à l'aide du masque d'adresse s'effectue en tenant compte du schéma (http ou https) :

   - S'il n'y a pas de protocole réseau dans le masque d'adresse, alors une adresse avec n'importe quel protocole réseau relève du masque d'adresse.

     Exemple : le masque d'adresse `example.com` comprend les adresses `http://example.com` et `https://example.com`.

   - Si un protocole réseau est présent dans le masque d'adresse, seules les adresses ayant le même protocole réseau que le masque d'adresse sont couvertes par le masque d'adresse.

     Exemple : le masque d'adresse `http://*.example.com` est soumis à l'adresse `http://www.example.com`, mais pas à l'adresse `https://www.example.com`.

9. Un masque d'adresse entre guillemets est traité sans tenir compte d'éventuelles substitutions supplémentaires, à l'exception du caractère `*`, s'il est initialement inclus dans le masque d'adresse. Pour les masques d'adresse entre guillemets doubles, les règles 5 et 7 ne sont pas suivies (voir les exemples 14 à 18 dans le tableau ci-dessous).

10. Lors de la comparaison avec un masque d'adresse de ressource Web, le nom d'utilisateur et le mot de passe, le port de connexion et la casse des caractères ne sont pas pris en compte.

Exemples d'application des règles de génération des masques d'adresses

Non.	Masque d'adresse	Adresse vérifiée de la ressource Web	L'adresse vérifiée satisfait-elle au masque d'adresse ?	Commentaire
1	*.example.com	http://www.123example.com	Non	Cf. règle 1.
2	*.example.com	http://www.123.example.com	Oui	Cf. règle 2.
3	*example.com	http://www.123example.com	Oui	Cf. règle 1.
4	*example.com	http://www.123.example.com	Oui	Cf. règle 1.
5	http://www.*.example.com	http://www.123example.com	Non	Cf. règle 1.
6	www.example.com	http://www.example.com	Oui	Voir règles 3, 2, 1.
7	www.example.com	https://www.example.com	Oui	Voir règles 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Oui	Voir règles 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Oui	Voir règles 3, 5, 1.
10	example.com	http://www.example.com	Oui	Voir règles 3, 1.
11	http://example.com/	http://example.com/abc	Oui	Cf. règle 6.
12	http://example.com/*	http://example.com	Oui	Cf. règle 7.
13	http://example.com	https://example.com	Non	Cf. règle 8.
14	"example.com"	http://www.example.com	Non	Cf. règle 9.
15	"http://www.example.com"	http://www.example.com/abc	Non	Cf. règle 9.
16	"*.example.com"	http://www.example.com	Oui	Voir règles 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Oui	Voir règles 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Oui	Voir règles 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Non	Le masque d'adresse contient plus d'informations que l'adresse de la ressource Web.

Contrôle des applications

Le Contrôle des applications gère le lancement des applications tierces sur les appareils des utilisateurs. Cela réduit le risque d'infection par une application malveillante sur l'appareil protégé.

Pour utiliser le module, vous devez posséder la licence qui couvre cette fonction.

Fonctionnement du Contrôle des applications

1. **L'utilisateur tente de lancer une application tierce**
2. **Le Contrôle des applications applique les règles**

   Le Contrôle des applications applique de manière séquentielle des règles à l'application en cours de lancement. Selon le mode de règle sélectionné, le module *contrôle* les applications en cours de lancement ou *teste* les règles. Une règle d'interdiction a une priorité supérieure à une règle d'autorisation.
3. **Fin de l'analyse**

   Si les règles empêchent l'exécution de l'application, le module bloque le lancement de cette application et génère un événement *Le lancement de l'application est interdit*. En mode test, le module ne bloque pas le lancement de cette application et génère l'événement *Le lancement de l'application est interdit en mode test*.

Configuration du Contrôle des applications

1. **Dresser l'inventaire des applications**

   Utilisez la tâche Inventaire pour obtenir la liste des applications installées sur les appareils protégés. Sur la base de ces informations, créez la liste des applications dont vous souhaitez empêcher l'exécution.
2. **Sélectionner le mode de fonctionnement du Contrôle des applications**

   Le module Contrôle des applications peut fonctionner dans l'un des deux modes suivants :

   - *Autoriser tout ce qui ne figure pas dans la liste des règles*. Le Contrôle des applications permet aux utilisateurs de lancer n'importe quelle application tierce, à l'exception de celles qui sont interdites par les règles.
   - *Bloquer tout ce qui ne figure pas dans la liste des règles*. Le Contrôle des applications permet aux utilisateurs de lancer n'importe quelle application tierce, à l'exception de celles qui sont autorisées et non interdites par les règles.

   Le choix du mode du Contrôle des applications dépend de la stratégie de sécurité de votre organisation, ainsi que du nombre d'applications que vous souhaitez contrôler.
3. **Créer des catégories d'applications**

Définissez les catégories d'applications autorisées ou interdites. Les catégories d'applications sont destinées à tous les appareils du réseau de l'organisation, quels que soient les groupes d'administration. Les catégories d'applications permettent de configurer des règles pour un groupe d'applications au lieu de les configurer selon des conditions d'inclusion et d'exclusion.

Il est conseillé de créer une catégorie "Applications pour le travail" qui reprend la sélection standard d'applications utilisées dans l'entreprise. Si différents groupes d'utilisateurs utilisent différentes sélections d'applications, vous pouvez créer une catégorie d'applications distincte pour chaque groupe d'utilisateurs.

Nous vous recommandons de configurer les catégories d'applications dans Kaspersky Security Center.

4. **Configurer les règles du Contrôle des applications**

   Le module contrôle le lancement des applications selon les *règles du Contrôle des applications*, qui définissent les conditions dans lesquelles le Contrôle des applications autorise ou interdit le lancement d'une application tierce pour un groupe d'utilisateurs sélectionné.

5. **Test des règles du Contrôle des applications**

   Par défaut, le contrôle des applications est désactivé. Nous vous recommandons d'activer le Contrôle des applications en mode test et de tester les règles du Contrôle des applications créées. L'application ne bloquera pas le lancement des applications tierces, mais enverra au Serveur d'administration des notifications concernant leur lancement.

6. **Découvrir le fonctionnement des règles du Contrôle des applications**

   Consultez le rapport sur le fonctionnement du Contrôle des applications en mode test. Après avoir examiné les informations, ajustez vos règles du Contrôle des applications si nécessaire.

7. **Activer l'utilisation des règles du Contrôle des applications**

   Dans ce mode, Kaspersky Endpoint Security empêche l'exécution d'applications tierces si les règles n'autorisent pas le lancement de ces applications.

   Comment activer l'utilisation des règles du Contrôle des applications dans la Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.
   4. Passez à la section **Contrôles de sécurité → Contrôle des applications**.
   5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
   6. Dans la section **Action lors du démarrage des applications**, sélectionnez l'action **Appliquer les règles** pour le Contrôle des applications.
   7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

   Comment activer l'utilisation des règles du Contrôle des applications via la ligne de commande

   Pour sélectionner le mode test pour le Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

L'administrateur de Kaspersky Security Center ou un utilisateur local avec le rôle admin attribué dans l'application peut interdire ou autoriser l'exécution de processus sous le compte root à l'aide de Contrôle des applications.

Considérations particulières et limitations

- Le Contrôle des applications ne prend pas en charge le contrôle de lancement des applications Snap, Flatpak et AppImage.
- Contrôle des applications ne contrôle pas le lancement des scripts depuis des interprètes qui ne sont pas compatibles avec Kaspersky Endpoint Security, ni le lancement des scripts transmis à l'interprète par une méthode autre que la ligne de commande. Kaspersky Endpoint Security prend en charge les interprètes suivants : python, perl, bash, ssh.
- Si les règles autorisent l'exécution de l'interpréteur, le Contrôle des applications ne bloque pas le lancement d'un script depuis cet interpréteur. Si le lancement d'au moins un script indiqué dans la ligne de commande de l'interpréteur est interdit par les règles, Kaspersky Endpoint Security bloque tous les scripts indiqués dans la ligne de commande de l'interpréteur. Exclusion : cat script.py | python.

Inventaire des applications

Pour créer des règles du Contrôle des applications optimales, il est recommandé de commencer par identifier les applications utilisées sur les appareils protégés du réseau local de l'entreprise. La tâche *Inventaire* permet d'obtenir les informations suivantes :

- Le nom et la version de l'application tierce
- Une brève description

Pour utiliser la tâche, vous devez posséder la licence qui couvre cette fonction.

Les bases de données de l'application Kaspersky Security Center peuvent conserver les informations relatives à 150 000 fichiers traités. Une fois la limite atteinte, les nouveaux fichiers ne seront pas traités. Pour reprendre l'inventaire, vous devez supprimer de l'appareil protégé les fichiers qui ont été ajoutés à la base de données de Kaspersky Security Center lors de l'inventaire précédent.

Configuration et exécution de la tâche d'inventaire

1. **Créer une tâche d'Inventaire**

   Comment créer une tâche d'inventaire dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

      La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux 12.5**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Inventory**.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la tâche.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche.

5. Quittez l'Assistant.

Comment créer une tâche d'inventaire sur la ligne de commande

Pour créer une tâche, exécutez la commande suivante :

```
kesl-control --create-task <task name> --type InventoryScan
```

où `<task name>` est le nom de la nouvelle tâche.

Cette commande renvoie l'ID de la tâche créée.

Exemple de résultat de l'exécution de la commande :

Tâche créée (ID de tâche : 100)

2 Configurer les zones d'inventaire

Il faut définir au moins une zone d'inventaire pour que la tâche puisse démarrer. Par défaut, la zone *Commandes exécutables* – `/usr/bin` est définie.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Comment configurer une zone d'inventaire dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche Inventaire créée.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zones d'inventaire**.

5. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'inventaire s'ouvre.

6. Dans le champ **Nom de la zone**, saisissez un nom pour la zone d'inventaire, par exemple *Fichiers sur le bureau*.

7. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire, par exemple `/path/to/folder`. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

8. Le cas échéant, indiquez des masques pour les noms d'objets au format d'interpréteur de commandes, par exemple, `*.txt`, `file?.*`. Ajoutez les masques un par un.

9. Enregistrez vos modifications.

Comment configurer une zone d'inventaire sur la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les paramètres actuels, exécutez la commande suivante :

```
kesl-control --get-settings <task name | task ID>
```

Symboles

Paramètres de la tâche d'inventaire

Paramètre	Description
`UseScanArea=Yes`	Activation d'une zone d'inventaire avec l'ID `#`. Vous pouvez désactiver temporairement l'analyse d'une zone d'inventaire au lieu de supprimer la zone. Pour ce faire, définissez `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description de la zone d'inventaire. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.
`AreaMask.item_#`	Restriction de la zone d'inventaire. Dans la zone d'inventaire, l'application analyse uniquement les objets indiqués à l'aide de masques au format de l'interpréteur de commandes. Vous pouvez définir plusieurs éléments `ScanScope.item_#.AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Par exemple, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. Valeur par défaut : `/usr/bin`

3 Si nécessaire, modifiez les paramètres de la tâche

Configuration de la tâche d'inventaire dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche Inventaire créée.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres de l'inventaire**.

5. Sélectionnez une action pour la catégorie d'applications « Golden Image » :

   - **Aucune modification** – ne pas modifier la catégorie Image système une fois l'inventaire terminé. Il s'agit de la sélection par défaut. Cette option est utilisée lorsque vous souhaitez obtenir la liste des applications tierces utilisées sur l'appareil, sans les ajouter à la catégorie « Image système ».

   - **Mise à jour ou création (si elle n'existe pas)** – ajoute les applications détectées sur l'appareil par la tâche d'inventaire à la catégorie « Image système ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour.

   - **Supprimer** – effacer la catégorie d'applications Image système. La catégorie est effacée dès le lancement de la tâche, sans effectuer d'inventaire des fichiers sur l'appareil.

6. Si nécessaire, cochez les cases suivantes :

   - **Inventaire des fichiers de scripts**. Rechercher les scripts dans la zone d'inventaire. L'application envoie ces informations à Kaspersky Security Center.

   - **Analyser tous les fichiers exécutables**.

   - **Analyser les fichiers binaires**. Analyse des fichiers binaires (fichiers avec les extensions .elf, .java et .pyc).

7. Enregistrez vos modifications.

Configuration de la tâche d'inventaire à partir de la ligne de commande

Exécutez la commande :

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

Symboles

Paramètres de la tâche d'inventaire

Paramètre	Description
`ScanScripts`	Rechercher les scripts dans la zone d'inventaire : `Yes` (valeur par défaut) : analyser les scripts. `No` : ne pas analyser les scripts.
`ScanBinaries`	Analyse des fichiers binaires (fichiers avec les extensions .elf, .java et .pyc) : `Yes` (valeur par défaut) : analyser les fichiers binaires. `No` : ne pas analyser les fichiers binaires.
`ScanAllExecutable`	Analyse des fichiers exécutables : `Yes` (valeur par défaut) : analyser les fichiers avec un bit exécutable. `No` : ne pas analyser les fichiers avec un bit exécutable.
`GoldenImageAction`	L'action que Kaspersky Endpoint Security doit effectuer sur la catégorie d'applications Golden Image à la fin de la tâche d'inventaire : `DoNothing` (par défaut) – ne modifiez pas la catégorie d'applications Golden Image. `Create` : ajouter les applications détectées à la catégorie d'applications « Golden Image ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. `Remove` – effacez la catégorie d'applications Golden Image. La catégorie est effacée dès le lancement de la tâche, sans effectuer d'inventaire des fichiers sur l'appareil.

4 Configurer des zones d'exclusion

Une exclusion a une priorité supérieure à celle d'une zone d'inventaire. Un objet exclu n'est pas analysé, même s'il se trouve dans une zone d'inventaire. Si la zone d'inventaire est définie à un niveau inférieur à celui du répertoire exclu, l'application ignore cette zone d'inventaire lors de l'exécution de la tâche.

Comment configurer une zone d'exclusion dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
2. La liste des tâches s'ouvre.
3. Cliquez sur la tâche Inventaire créée.

   La fenêtre des propriétés de la tâche s'ouvre.
4. Sélectionnez l'onglet **Paramètres de l'application**.
5. Passez à la section **Zones d'exclusion**.
6. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'exclusion s'ouvre.
7. Dans le champ **Nom de la zone**, indiquez le nom de la zone d'exclusion, par exemple *Fichiers système*.
8. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
9. Spécifiez les masques de noms d'objets au format de l'interpréteur de commandes (par exemple `*.txt` ou `file?.*`). Ajoutez les masques un par un.
10. Enregistrez vos modifications.

Comment configurer une zone d'exclusion sur la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les paramètres actuels, exécutez la commande suivante :

```
kesl-control --get-settings <task name | task ID>
```

Symboles

Paramètres de la tâche d'inventaire

Paramètre	Description
`UseScanArea`	Exclusion de la zone d'inventaire indiquée. Vous pouvez désactiver temporairement une zone d'exclusion au lieu de la supprimer. Pour ce faire, définissez `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description de la zone d'exclusion de l'inventaire.

Paramètre	Description
`AreaMask.item_#`	Restriction de la zone d'exclusion. Dans la zone d'exclusion, l'application exclut des analyses uniquement les objets indiqués à l'aide de masques au format de l'interpréteur de commandes. Vous pouvez définir plusieurs éléments `ExcludedFromScanScope.item_#.AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Par exemple, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Chemin d'accès au répertoire à exclure de l'inventaire. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exemple d'exclusion du répertoire `/tmp` de l'inventaire :

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5. **Lancement de la tâche**

Comment lancer la tâche Inventaire dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cochez la case en regard de la tâche créée.

3. Cliquez sur **Démarrer**.

Comment lancer une tâche Inventaire en ligne de commande

Pour lancer la tâche, exécutez la commande suivante :

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `[-W]` : activer la sortie des événements actuels liés à cette tâche.
- `[--progress]` : activer l'affichage de la progression de la tâche.

Consultation de la liste des applications détectées

Pour consulter, dans la Web Console, la liste des applications détectées sur les appareils :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche Inventaire créée.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Résultats**.

Consulter la liste des applications détectées sur l'appareil client

```
kesl-control --get-app-list [--json]
```

Kaspersky Endpoint Security affiche les informations suivantes sur les applications détectées :

- Date et heure de l'inventaire
- Nombre d'applications
- Liste des applications contenant les informations suivantes :
  - Chemin d'accès à l'application.
  - La somme de hash de l'application.
  - Type d'application. Par exemple : `Script`, `Executable`.
  - Les catégories auxquelles l'application appartient (si elles ont été créées auparavant). Vous pouvez consulter la liste des catégories d'applications créées à l'aide de la commande suivante :

    ```
    kesl-control --get-categories
    ```

Lorsqu'une nouvelle catégorie est ajoutée, ses informations dans la liste des applications ne sont pas automatiquement mises à jour. Pour mettre à jour la liste des applications, vous devez relancer la tâche Inventaire.

Comment configurer le mode de fonctionnement du Contrôle des applications

Le module Contrôle des applications peut fonctionner dans l'un des deux modes suivants :

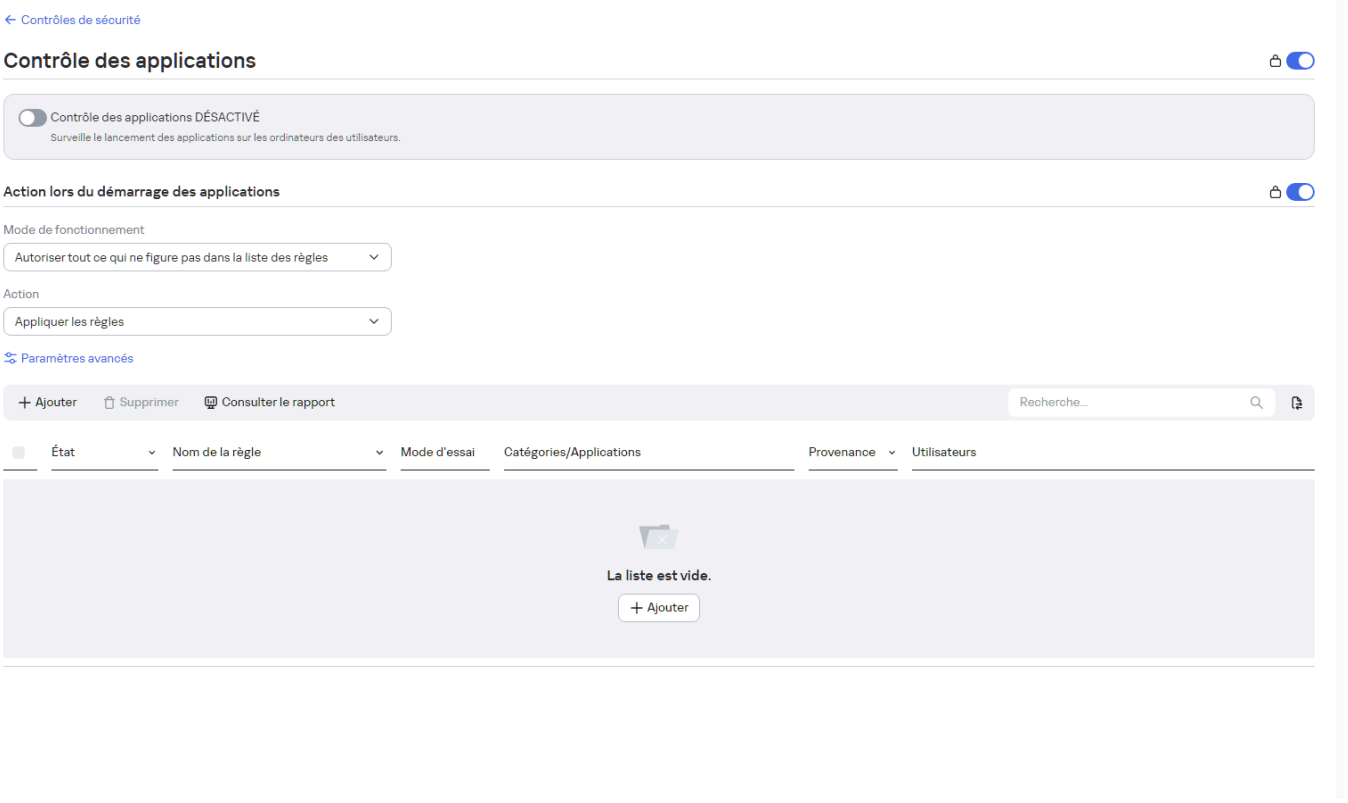
- *Autoriser tout ce qui ne figure pas dans la liste des règles*. Le Contrôle des applications permet aux utilisateurs de lancer n'importe quelle application tierce, à l'exception de celles qui sont interdites par les règles.
- *Bloquer tout ce qui ne figure pas dans la liste des règles*. Le Contrôle des applications permet aux utilisateurs de lancer n'importe quelle application tierce, à l'exception de celles qui sont autorisées et non interdites par les règles.

Le choix du mode du Contrôle des applications dépend de la stratégie de sécurité de votre organisation, ainsi que du nombre d'applications que vous souhaitez contrôler.

Comment configurer le mode de fonctionnement du Contrôle des applications dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
6. Sous **Action lors du démarrage des applications**, sélectionnez le mode de fonctionnement du Contrôle des applications :
   - **Autoriser tout ce qui ne figure pas dans la liste des règles**
   - **Bloquer tout ce qui ne figure pas dans la liste des règles**
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Contrôle des applications

Comment configurer le mode de fonctionnement du Contrôle des applications en ligne de commande

Exécutez la commande :

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

Symboles

Paramètre	Description
`AppControlMode`	`AllowList` : Kaspersky Endpoint Security interdit pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. `DenyList` (valeur par défaut) : Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.

Création des catégories d'applications.

Pour simplifier la création de règles de Contrôle des applications, vous pouvez créer des *catégories d'applications*.

Kaspersky Endpoint Security détermine la catégorie d'une application à l'aide des technologies suivantes :

- Bases antivirus.
- Services cloud de Kaspersky Security Network.
- La technologie d'analyse heuristique permet de détecter les menaces qui ne sont pas encore couvertes par les bases de Kaspersky.

Dans Kaspersky Endpoint Security for Linux, les catégories peuvent être créées en fonction des paramètres suivants :

- nom du fichier exécutable de l'application ;
- nom du dossier contenant le fichier exécutable de l'application ;
- hachage du fichier exécutable de l'application. Seul SHA256 est autorisé.

  Vous pouvez utiliser des masques pour définir les noms des fichiers et des répertoires.

  Règles de définition des masques

  Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

  Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

  Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Il est conseillé de créer une catégorie "Applications pour le travail" qui reprend la sélection standard d'applications utilisées dans l'entreprise. Si différents groupes d'utilisateurs utilisent différentes sélections d'applications, vous pouvez créer une catégorie d'applications distincte pour chaque groupe d'utilisateurs.

Kaspersky Endpoint Security for Linux ne prend pas en charge les catégories KL.

Pour créer une catégorie d'applications dans Kaspersky Security Center :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Applications tierces → Catégories d'applications**.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de catégories personnalisée s'ouvre.

3. Suivez les instructions de l'Assistant de création de catégories personnalisées.

Étape 1.

À cette étape, indiquez le nom de la catégorie d'applications et choisissez l'un des types de catégories d'applications suivants :

- *Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie*. Si vous avez choisi ce type de catégorie, aux étapes *Conditions* et *Exclusions*, vous pourrez définir les critères d'inclusion des fichiers exécutables dans la catégorie.

- *Catégorie qui reprend les fichiers exécutables d'un dossier particulier. Les fichiers exécutables des applications copiés dans ce dossier particulier sont traités automatiquement et leurs métriques sont ajoutées à la catégorie*. Si vous avez sélectionné ce type de catégorie, vous pourrez à l'étape suivante indiquer le dossier dont les fichiers exécutables seront automatiquement inclus dans la catégorie.

- *Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés. Ces fichiers exécutables sont traités automatiquement et leurs métriques sont ajoutées à la catégorie*. Si vous avez choisi ce type de catégorie, vous pourrez à l'étape suivante désigner l'ordinateur dont les fichiers exécutables seront automatiquement repris dans la catégorie.

Étape 2.

Cette étape est disponible si vous avez sélectionné le type de catégorie suivant : **Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie**.

Sélectionnez à cette étape les critères d'inclusion des applications dans la catégorie :

- **De la catégorie KL**

  Si cette option est sélectionnée, vous pouvez définir une catégorie d'applications Kaspersky comme condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.

  Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.

- **Sélectionnez le certificat dans le référentiel**

  Si cette option est sélectionnée, vous pouvez indiquer les certificats du magasin. La condition de catégorie ne s'applique qu'aux fichiers exécutables signés avec le certificat indiqué.

  Si vous avez sélectionné un certificat comme condition de déclenchement des règles, assurez-vous que ce certificat est ajouté au stockage système sécurisé sur l'ordinateur et vérifiez les paramètres d'utilisation du stockage système sécurisé dans l'application.

- **Définir le chemin d'accès à l'application (masques pris en charge)**

  Si cette option est sélectionnée, vous pouvez indiquer un fichier ou un dossier sur l'appareil client, à partir duquel les fichiers exécutables seront ajoutés à la catégorie d'applications personnalisées. Vous pouvez utiliser des expressions régulières, comme `C:\path_to_exe\*`, par exemple : `C:\Program Files\Internet Explorer\*`.

- **Disque amovible**

  Si cette option est sélectionnée, vous pouvez indiquer le type de support (tout support ou support amovible) à partir duquel l'application est lancée. Les applications lancées à partir de supports du type sélectionné sont ajoutées à la catégorie d'applications personnalisées.

- **Hash, métadonnées ou certificat** :

  - **Sélectionner dans la liste des fichiers exécutables**

    Si cette option est sélectionnée, vous pouvez sélectionner les applications à ajouter à la catégorie à partir de la liste des fichiers exécutables sur l'appareil client.

  - **Sélectionner dans le registre des applications**

    Si cette option est sélectionnée, le registre des applications s'affiche. Après avoir sélectionné une application dans le registre, une fenêtre s'ouvre contenant des paramètres préremplis avec les métadonnées de l'application sélectionnée :

    - Nom du fichier
    - Version du fichier Vous pouvez définir une version exacte ou saisir une condition, par exemple, "supérieure à 5.0".
    - Le nom de l'application.
    - Version de l'application. Vous pouvez définir une version exacte ou saisir une condition, par exemple, "ultérieure à 5.0".
    - Éditeur.

    Notez que seuls les fichiers exécutables correspondant aux paramètres définis sont bloqués, mais pas le lancement de l'application sélectionnée en tant que telle. Si les métadonnées sélectionnées correspondent aux métadonnées du fichier exécutable qui est lancé lorsque vous démarrez l'application, vous pouvez passer à l'étape suivante. Sinon, vous devez modifier les valeurs manuellement pour les faire correspondre aux métadonnées du fichier exécutable.

- **Définir manuellement**

  Si cette option est sélectionnée, vous devez définir un hachage de fichier, des métadonnées ou un certificat comme condition d'ajout d'applications à une catégorie personnalisée.

  Hachage du fichier

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, vous devez sélectionner un algorithme de hachage que Kaspersky Endpoint Security applique aux fichiers de la catégorie. Les informations sur les valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

  SHA256 est une fonction de hachage cryptographique dont l'algorithme ne présente aucune faiblesse connue. Elle est actuellement considérée comme étant la forme de hachage la plus sûre. Kaspersky Endpoint Security 10 et les versions ultérieures prennent en charge l'algorithme SHA256. La fonction de hachage MD5 est prise en charge pour les versions de Kaspersky Endpoint Security antérieures à la version 10.

  Sélectionnez une des fonctions de hachage que Kaspersky Endpoint Security doit appliquer aux fichiers de la catégorie :

  - Si toutes les instances des applications de sécurité installées dans votre réseau sont des versions 10 ou ultérieures de Kaspersky Endpoint Security, cochez la case **SHA256**. Nous ne recommandons pas de créer une catégorie basée sur le hachage SHA256 du fichier exécutable de Kaspersky Endpoint Security 10 ou de toute version antérieure. Des dysfonctionnements de l'application de sécurité peuvent en résulter. Dans ce cas, vous pouvez utiliser la fonction de hachage cryptographique MD5 pour les fichiers de la catégorie.

  - Si des versions antérieures à Kaspersky Endpoint Security 10 sont installées sur votre réseau, cochez la case **Hash MD5**. Il n'est pas possible d'ajouter une catégorie basée sur le hachage MD5 du fichier exécutable pour Kaspersky Endpoint Security 10 ou une version ultérieure. Dans ce cas, vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

  - Si votre réseau comprend des appareils qui utilisent des versions de Kaspersky Endpoint Security antérieures ou ultérieures à la version 10, cochez les cases **SHA256** et **Hash MD5**.

  Données méta

  Si cette option est sélectionnée, vous pouvez indiquer les métadonnées du fichier, comme le nom du fichier, la version du fichier et le fournisseur. Une condition de catégorie ne concerne que les fichiers exécutables dont les métadonnées sont identiques.

  Certificat

  Si cette option est sélectionnée, vous pouvez indiquer les certificats du magasin. La condition de catégorie ne s'applique qu'aux fichiers exécutables signés avec le certificat indiqué.

- **À partir du dossier MSI/d'archives**

  Si cette option est sélectionnée, vous pouvez définir un fichier d'installation MSI comme condition d'ajout d'applications à la catégorie personnalisée. Les métadonnées du programme d'installation de l'application sont envoyées au Serveur d'administration. Les applications dont les métadonnées du programme d'installation correspondent au programme d'installation MSI indiqué sont ajoutées à la catégorie des applications personnalisées.

Étape 3.

Cette étape est disponible si vous avez sélectionné le type de catégorie suivant : **Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie**.

Les applications renseignées à cette étape sont exclues de la catégorie, même si ces applications avaient été renseignées à l'étape "Configuration des conditions d'inclusion des applications dans une catégorie".

À cette étape, sélectionnez les critères d'exclusion des applications de la catégorie :

- **De la catégorie KL**

  Si cette option est sélectionnée, vous pouvez définir une catégorie d'applications Kaspersky comme condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.

  Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.

- **Sélectionnez le certificat dans le référentiel**

  Si cette option est sélectionnée, vous pouvez indiquer les certificats du magasin. La condition de catégorie ne s'applique qu'aux fichiers exécutables signés avec le certificat indiqué.

  Si vous avez sélectionné un certificat comme condition de déclenchement des règles, assurez-vous que ce certificat est ajouté au stockage système sécurisé sur l'ordinateur et vérifiez les paramètres d'utilisation du stockage système sécurisé dans l'application.

- **Définir le chemin d'accès à l'application (masques pris en charge)**

  Si cette option est sélectionnée, vous pouvez indiquer un fichier ou un dossier sur l'appareil client, à partir duquel les fichiers exécutables seront ajoutés à la catégorie d'applications personnalisées. Vous pouvez utiliser des expressions régulières, comme `C:\path_to_exe\*`, par exemple : `C:\Program Files\Internet Explorer\*`.

- **Disque amovible**

  Si cette option est sélectionnée, vous pouvez indiquer le type de support (tout support ou support amovible) à partir duquel l'application est lancée. Les applications lancées à partir de supports du type sélectionné sont ajoutées à la catégorie d'applications personnalisées.

- **Hash, métadonnées ou certificat** :

  - **Sélectionner dans la liste des fichiers exécutables**

    Si cette option est sélectionnée, vous pouvez sélectionner les applications à ajouter à la catégorie à partir de la liste des fichiers exécutables sur l'appareil client.

- **Sélectionner dans le registre des applications**

  Si cette option est sélectionnée, le registre des applications s'affiche. Après avoir sélectionné une application dans le registre, une fenêtre s'ouvre contenant des paramètres préremplis avec les métadonnées de l'application sélectionnée :

  - Nom du fichier
  - Version du fichier Vous pouvez définir une version exacte ou saisir une condition, par exemple, "supérieure à 5.0".
  - Le nom de l'application.
  - Version de l'application. Vous pouvez définir une version exacte ou saisir une condition, par exemple, "ultérieure à 5.0".
  - Éditeur.

  Notez que seuls les fichiers exécutables correspondant aux paramètres définis sont bloqués, mais pas le lancement de l'application sélectionnée en tant que telle. Si les métadonnées sélectionnées correspondent aux métadonnées du fichier exécutable qui est lancé lorsque vous démarrez l'application, vous pouvez passer à l'étape suivante. Sinon, vous devez modifier les valeurs manuellement pour les faire correspondre aux métadonnées du fichier exécutable.

- **Définir manuellement**

  Si cette option est sélectionnée, vous devez définir un hachage de fichier, des métadonnées ou un certificat comme condition d'ajout d'applications à une catégorie personnalisée.

  Hachage du fichier

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, vous devez sélectionner un algorithme de hachage que Kaspersky Endpoint Security applique aux fichiers de la catégorie. Les informations sur les valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

  SHA256 est une fonction de hachage cryptographique dont l'algorithme ne présente aucune faiblesse connue. Elle est actuellement considérée comme étant la forme de hachage la plus sûre. Kaspersky Endpoint Security 10 et les versions ultérieures prennent en charge l'algorithme SHA256. La fonction de hachage MD5 est prise en charge pour les versions de Kaspersky Endpoint Security antérieures à la version 10.

Sélectionnez une des fonctions de hachage que Kaspersky Endpoint Security doit appliquer aux fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées dans votre réseau sont des versions 10 ou ultérieures de Kaspersky Endpoint Security, cochez la case **SHA256**. Nous ne recommandons pas de créer une catégorie basée sur le hachage SHA256 du fichier exécutable de Kaspersky Endpoint Security 10 ou de toute version antérieure. Des dysfonctionnements de l'application de sécurité peuvent en résulter. Dans ce cas, vous pouvez utiliser la fonction de hachage cryptographique MD5 pour les fichiers de la catégorie.

- Si des versions antérieures à Kaspersky Endpoint Security 10 sont installées sur votre réseau, cochez la case **Hash MD5**. Il n'est pas possible d'ajouter une catégorie basée sur le hachage MD5 du fichier exécutable pour Kaspersky Endpoint Security 10 ou une version ultérieure. Dans ce cas, vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

- Si votre réseau comprend des appareils qui utilisent des versions de Kaspersky Endpoint Security antérieures ou ultérieures à la version 10, cochez les cases **SHA256** et **Hash MD5**.

Données méta

Si cette option est sélectionnée, vous pouvez indiquer les métadonnées du fichier, comme le nom du fichier, la version du fichier et le fournisseur. Une condition de catégorie ne concerne que les fichiers exécutables dont les métadonnées sont identiques.

Certificat

Si cette option est sélectionnée, vous pouvez indiquer les certificats du magasin. La condition de catégorie ne s'applique qu'aux fichiers exécutables signés avec le certificat indiqué.

- **À partir du dossier MSI/d'archives**

  Si cette option est sélectionnée, vous pouvez définir un fichier d'installation MSI comme condition d'ajout d'applications à la catégorie personnalisée. Les métadonnées du programme d'installation de l'application sont envoyées au Serveur d'administration. Les applications dont les métadonnées du programme d'installation correspondent au programme d'installation MSI indiqué sont ajoutées à la catégorie des applications personnalisées.

Étape 4. Paramètres

Cette étape est disponible si vous avez sélectionné le type de catégorie suivant : **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés. Ces fichiers exécutables sont traités automatiquement et leurs métriques sont ajoutées à la catégorie**.

À cette étape, cliquez sur le bouton **Ajouter** et indiquez les ordinateurs dont les fichiers exécutables seront ajoutés à la catégorie d'applications par Kaspersky Security Center.

À cette étape, configurez les paramètres suivants :

- **Algorithme de calcul de la fonction de hachage**

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, vous devez sélectionner l'algorithme de hachage que Kaspersky Security Center applique aux fichiers de la catégorie. Les informations sur les valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

  SHA256 est une fonction de hachage cryptographique dont l'algorithme ne présente aucune faiblesse connue ; elle est actuellement considérée comme la fonction de hachage la plus sûre. Kaspersky Endpoint Security for Linux prend en charge SHA256.

  Sélectionnez l'un des algorithmes de hachage à appliquer aux fichiers de la catégorie :

  - Si vous utilisez Kaspersky Endpoint Security for Linux sur les appareils protégés, cochez la case **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)**.

  - Si vous utilisez Kaspersky Endpoint Security for Windows sur les appareils protégés, cochez la case **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

  Si vous utilisez les applications pour Windows et Linux sur votre réseau, cochez les deux cases.

- **Synchroniser les données avec le stockage du Serveur d'administration**

  Sélectionnez cette option si vous souhaitez que le Serveur d'administration vérifie périodiquement si le dossier (ou les dossiers) défini(s) a (ont) été modifié(s).

  Le paramètre est désactivé par défaut.

  Si vous activez ce paramètre, indiquez la période en heures pendant laquelle le dossier (ou les dossiers) défini(s) est (sont) contrôlé(s) pour vérifier s'il(s) a (ont) été modifié(s). Par défaut, la période est fixée à 24 heures.

- **Type de fichiers**

  Dans cette section, vous pouvez indiquer le type de fichier que vous souhaitez utiliser pour créer la catégorie d'applications.

  tous les fichiers ;. La catégorie correspondra à tous les fichiers. Cette option est activée par défaut.

  Uniquement les fichiers hors des catégories d'applications. La catégorie correspondra uniquement aux fichiers ne faisant pas partie des catégories d'applications.

- **Dossiers**

  Dans cette section, vous pouvez spécifier les dossiers des ordinateurs sélectionnés qui contiennent les fichiers que vous souhaitez utiliser pour créer la catégorie d'applications.

  Tous les dossiers. La catégorie correspondra à tous les dossiers. Cette option est activée par défaut.

  Dossier indiqué. La catégorie correspondra uniquement au dossier spécifié. Si vous sélectionnez cette option, vous devez indiquer un chemin d'accès au dossier.

Étape 5.

Cette étape est disponible si vous avez sélectionné le type de catégorie suivant : **Catégorie qui reprend les fichiers exécutables d'un dossier particulier. Les fichiers exécutables des applications copiés dans ce dossier particulier sont traités automatiquement et leurs métriques sont ajoutées à la catégorie**.

À cette étape, indiquez le dossier dont les fichiers exécutables seront utilisés pour créer la catégorie.

Gérez les paramètres suivants :

- **Inclure dans la catégorie des bibliothèques connectées de manière dynamique (.DLL)**

  La catégorie d'applications inclut les bibliothèques de liens dynamiques (fichiers au format DLL), et le module Contrôle des applications consigne les actions de ces bibliothèques qui s'exécutent dans le système. Lorsque des fichiers DLL sont ajoutés à une catégorie d'applications, il se peut que les performances de Kaspersky Security Center diminuent.

  La case est décochée par défaut.

- **Inclure les données relatives aux scripts dans la catégorie**

  La catégorie d'applications inclut les données relatives aux scripts, et les scripts ne sont pas bloqués par la Protection contre les menaces Internet. L'inclusion des données des scripts dans la catégorie peut réduire les performances de Kaspersky Security Center.

  La case est décochée par défaut.

- **Algorithme de calcul de la fonction de hachage**

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, vous devez sélectionner l'algorithme de hachage que Kaspersky Security Center applique aux fichiers de la catégorie. Les informations sur les valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

  SHA256 est une fonction de hachage cryptographique dont l'algorithme ne présente aucune faiblesse connue ; elle est actuellement considérée comme la fonction de hachage la plus sûre. Kaspersky Endpoint Security for Linux prend en charge SHA256.

  Sélectionnez l'un des algorithmes de hachage à appliquer aux fichiers de la catégorie :

  - Si vous utilisez Kaspersky Endpoint Security for Linux sur les appareils protégés, cochez la case **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)**.

  - Si vous utilisez Kaspersky Endpoint Security for Windows sur les appareils protégés, cochez la case **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

  Si vous utilisez les applications pour Windows et Linux sur votre réseau, cochez les deux cases.

- **Analyse forcée du dossier à la recherche de la présence de modifications**

  Si cette option est activée, l'application vérifie régulièrement si le dossier d'ajout de contenu à la catégorie a été modifié. Vous pouvez indiquer la fréquence des vérifications (en heures) dans le champ de saisie situé en regard de la case. Par défaut, l'intervalle entre les vérifications forcées est de 24 heures.

  Si cette option est désactivée, l'application n'effectue aucune vérification forcée du dossier. Le Serveur tente d'accéder aux fichiers s'ils ont été modifiés, ajoutés ou supprimés.

  La case est décochée par défaut.

Étape 6.

Quittez l'Assistant. Une fois l'Assistant terminé, la nouvelle catégorie d'applications est créée. Vous pouvez contrôler les applications de la catégorie à l'aide de règles de Contrôle des applications.

Image système

Vous pouvez utiliser l'Inventaire pour ajouter la catégorie d'applications Golden Image. Par défaut, la catégorie est vide. La catégorie « Image système » inclut les applications qui sont fournies sur l'appareil avec le système d'exploitation. Les applications de cette catégorie sont considérées comme fiables. Si nécessaire, vous pouvez ajouter des applications tierces à la catégorie.

Une fois la tâche d'Inventaire terminée, l'application peut modifier la catégorie « Image système » comme suit :

- **Aucune modification** – ne pas modifier la catégorie Image système une fois l'inventaire terminé. Il s'agit de la sélection par défaut. Cette option est utilisée lorsque vous souhaitez obtenir la liste des applications tierces utilisées sur l'appareil, sans les ajouter à la catégorie « Image système ».

- **Mise à jour ou création (si elle n'existe pas)** – ajoute les applications détectées sur l'appareil par la tâche d'inventaire à la catégorie « Image système ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour.

- **Supprimer** – effacer la catégorie d'applications Image système. La catégorie est effacée dès le lancement de la tâche, sans effectuer d'inventaire des fichiers sur l'appareil.

  Cela peut être utile dans les scénarios suivants :

  - Si vous devez empêcher le lancement d'applications de la catégorie « Image système » sur l'appareil, mais que vous ne pouvez pas désactiver la règle du Contrôle des applications.

  - Si vous appliquez une nouvelle stratégie à un appareil qui contient des règles du Contrôle des applications différentes de celles de la stratégie actuelle, ou lorsque vous déplacez un appareil vers une stratégie enfant. Dans ce cas, nous vous recommandons d'effacer la catégorie « Image système » afin d'éviter de bloquer par erreur des applications autorisées.

Configuration de la catégorie « Image système » à partir d'un ordinateur de référence

Vous pouvez utiliser un ordinateur de référence pour créer une catégorie « Image système » contenant l'ensemble d'applications dont vous avez besoin. Vous pouvez ensuite utiliser cette catégorie pour créer des règles d'autorisation du Contrôle des applications.

La configuration de la catégorie « Image système » à partir d'un ordinateur de référence comprend les étapes suivantes :

1. **Configurer un ordinateur de référence**

   Installez et configurez tous les logiciels nécessaires au fonctionnement des appareils sur le réseau de l'entreprise, y compris Kaspersky Endpoint Security for Linux et l'Agent d'administration.

2. **Créer une tâche d'Inventaire**

   Créez la tâche dans la Web Console ou en ligne de commande et configurez les paramètres suivants :

   - Action avec la catégorie d'applications « Image système » : **Mise à jour ou création (si elle n'existe pas)**;

     ```
     GoldenImageAction=Create
     ```

   - La zone d'inventaire est l'ordinateur de référence.

3. **Exécutez la tâche d'Inventaire et attendez qu'elle se termine.**

   La tâche génère la catégorie d'applications « Image système ».

4. **Exporter la liste des catégories dans un fichier.**

   > Vous ne pouvez pas exporter de liste de catégories dans la Web Console.

   Exécutez la commande :

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   Où `<path to file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de la tâche.

5. **Si nécessaire, ajuster votre catégorie « Image système »**

   Vérifiez le fichier de configuration contenant la liste des catégories d'applications. Si nécessaire, ajustez la liste des applications dans la catégorie « Image système ».

6. **Importer les paramètres depuis le fichier de configuration.**

   Si vous avez modifié le fichier de configuration contenant la liste des catégories d'applications, importez-le dans l'application :

   ```
   kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
   ```

   où `<category name 1> <category name 2> ... <category name N>` sont les noms des catégories autres que la catégorie « Image système » dont vous souhaitez modifier les informations.

   `<path to file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de la tâche.

Ainsi, vous pouvez utiliser la catégorie « Image système » pour créer des règles du Contrôle des applications.

À propos des règles du contrôle des applications

Une *règle du Contrôle des applications* est un ensemble de conditions qui déterminent si le Contrôle des applications autorise ou interdit le lancement d'une application tierce pour un groupe d'utilisateurs sélectionné.

Les règles limitent le lancement d'applications tierces selon les critères suivants :

- **Catégories d'applications**. L'application appartenant à la catégorie d'applications.

  > Vous ne pouvez utiliser une catégorie dans une seule règle.

- **Utilisateurs et groupes d'utilisateurs**. Le Contrôle des applications permet de limiter l'accès aux applications tierces pour des utilisateurs individuels ou des groupes d'utilisateurs. Par exemple, vous pouvez limiter l'accès aux applications d'administration à distance pour tous les utilisateurs de l'organisation, à l'exception de ceux du service informatique.

Les règles du Contrôle des applications peuvent avoir l'un des *états de fonctionnement* suivants :

- **Activée.** Le Contrôle des applications applique la règle.
- **Désactivé**. Le Contrôle des applications n'applique pas la règle.
- **Test**. Le Contrôle des applications ne bloquera pas l'exécution des applications tierces, mais enverra des notifications concernant leur lancement au Serveur d'administration.

Comment ajouter des règles du Contrôle des applications dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité → Contrôle des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.

6. Cliquez sur le bouton **Ajouter** dans le groupe **Action lors du démarrage des applications**.

   Cette action ouvre le formulaire d'ajout d'une règle du Contrôle des applications.

7. Dans le champ **État**, définissez l'état de la règle.

8. Pour tester la règle, placez ce commutateur sur **Activé** et cochez la case **Mode d'essai**.

9. Dans le champ **Nom de la règle**, saisissez le nom de la règle. Le nom de la règle doit être unique.

10. Sélectionnez la catégorie d'applications à laquelle vous souhaitez appliquer la règle. Il est impossible d'enregistrer une règle sans spécifier de catégorie.

11. Sélectionnez les utilisateurs ou le groupe d'utilisateurs ainsi que leurs autorisations d'exécution des applications.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter des règles du Contrôle des applications via la ligne de commande

1. Exportez la liste des règles du Contrôle des applications dans un fichier :

   ```
   kesl-control --get-settings 21 --file <path to file> [--json]
   ```

2. Ouvrez le fichier de configuration et ajoutez une section pour la règle avec l'ID `#`, en fonction du mode du Contrôle des applications :

   a. Si le mode `AppControlMode=AllowList`:

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   est sélectionné

   b. Si le mode `AppControlMode=DenyList`:

   ```
   [DenyListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [DenyListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   est sélectionné

3. Importez les paramètres du fichier de configuration dans l'application :

   ```
   kesl-control --set-settings 21 --file <path to file> [--json]
   ```

Symboles

Options de la commande

Paramètre	Description
`[AllowListRules.item_#]` `[DenyListRules.item_#]`	Règle du Contrôle des applications avec l'ID `#`.
`[AllowListRules.item_#.ACL.item_#]` `[DenyListRules.item_#.ACL.item_#]`	Liste des utilisateurs auxquels s'applique la règle du Contrôle des applications avec l'ID `#`.
`Description`	Description de la règle du Contrôle des applications.
`AppControlRuleStatus`	État de fonctionnement de la règle du Contrôle des applications. `On` (valeur par défaut) : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le Contrôle des applications. `Off` : la règle n'est pas utilisée pour contrôler les applications. `Test` : l'application Kaspersky Endpoint Security autorise le lancement des applications soumises à l'action de la règle, mais consigne les informations relatives au lancement de ces applications dans le rapport.
`Category`	Nom de la catégorie des applications à laquelle la règle s'applique. Vous pouvez spécifier la catégorie `Golden Image`.
`Access`	Type d'accès attribué à un utilisateur ou à un groupe d'utilisateurs : `Allow` (valeur par défaut) : autorise le lancement d'applications. `Block` : interdit le lancement d'applications.
`Principal`	Utilisateur ou groupe d'utilisateurs auquel s'applique la règle du Contrôle des applications : `\Everyone` (valeur par défaut) : la règle s'applique à tous les utilisateurs. `<user>` est le nom de l'utilisateur auquel la règle s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle s'applique.

Mode de test des règles du Contrôle des applications

Pour garantir que le Contrôle des applications ne bloque pas les applications nécessaires au fonctionnement, il est recommandé de tester les règles du Contrôle des applications. Dans le mode test, Kaspersky Endpoint Security bloquera l'exécution des applications tierces et enverra des notifications sur leur lancement au Serveur d'administration.

Par défaut, le Contrôle des applications autorise l'exécution de toutes les applications tierces, sauf celles interdites par les règles.

Test des règles du Contrôle des applications

1. **Créer les règles du Contrôle des applications**

   Configurez et activez les règles du Contrôle des applications que vous souhaitez tester. Par exemple, vous pouvez créer des règles qui empêchent l'exécution de toutes les applications tierces, à l'exception des applications des catégories « Image de référence » et « Applications de travail ».

2. **Activer le Contrôle des applications en mode test**

   Comment activer le mode de test du Contrôle des applications dans la Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité → Contrôle des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
6. Dans la section **Action lors du démarrage des applications**, sélectionnez l'action **Informer** pour le Contrôle des applications.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer le mode de test du Contrôle des applications sur la ligne de commande

Pour sélectionner le mode test pour le Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 AppControlRulesAction=TestRules
```

3 Examiner les résultats du test

Examinez le rapport du Contrôle des applications et les événements du module envoyés à Kaspersky Security Center.

Comment consulter le rapport du Contrôle des applications dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité → Contrôle des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
6. Dans le tableau des règles du Contrôle des applications, cliquez sur le bouton **Consulter le rapport**.
7. La fenêtre **Rapport sur les applications interdites en mode test** s'ouvre.
8. Examinez les informations relatives au lancement des applications interdites en mode test.

Comment consulter les événements résultant d'un fonctionnement test du Contrôle des applications

1. Dans la fenêtre principale de Web Console, sélectionnez **Surveillance → Sélections d'événements**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Nouvelle sélection d'événements** qui s'ouvre, indiquez un nom pour la sélection. Par exemple, « Test des règles du Contrôle des applications ».
4. Accédez à la section **Événements** et gérez les paramètres suivants :
   - **Nom de l'application** – Kaspersky Endpoint Security for Linux.
   - **Niveau de gravité** – **Information**.

- Choisissez l'option **Inclure les événements généraux sélectionnés**.
- Cochez les cases en regard des événements **Le lancement de l'application est interdit en mode test** et **Le lancement de l'application est autorisé en mode test**.

5. Si nécessaire, configurez les autres paramètres.
6. Enregistrez vos modifications.
7. Cliquez sur le nom de la sélection pour consulter le résultat de la sélection d'événements.

4 **Ajuster les règles**

Si aucune des applications indispensables au travail de l'utilisateur de l'ordinateur n'affiche des événements d'interdiction de lancement en mode test, les règles créées sont correctes.

Dans le cas contraire, modifiez les paramètres des règles que vous avez créées, créez des règles supplémentaires ou supprimez les règles existantes.

Contrôle de l'intégrité du système

Le module Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Endpoint Security génère les événements correspondants et en informe l'administrateur.

Fonctionnement du Contrôle de l'intégrité du système

Le Contrôle de l'intégrité du système peut fonctionner en temps réel et à la demande :

- Le module *Contrôle de l'intégrité du système* vous permet de surveiller les modifications apportées aux fichiers et aux répertoires que vous avez inclus dans la zone de surveillance, *en temps réel*.
- La fonctionnalité *Vérification de l'intégrité du système* vous permet de comparer l'état actuel des objets inclus dans la zone de surveillance avec leur état enregistré, *selon une planification ou à la demande*.

Le module Contrôle de l'intégrité du système ne transmet pas de données sur les modifications exactes qui ont été apportées. La tâche *Vérification de l'intégrité du système* rapporte des informations sur les attributs modifiés et les fichiers et répertoires déplacés.

Considérations particulières et limitations

- Les restrictions technologiques du système d'exploitation Linux empêchent une application de déterminer quel utilisateur ou processus a apporté une modification à un fichier.
- Lors de l'ajout d'un répertoire à une zone de surveillance ou à une zone d'exclusion, l'application ne vérifie pas si le répertoire existe.

Surveillez l'intégrité du système en temps réel

Le Contrôle de l'intégrité du système permet de détecter en temps réel les modifications d'un objet inclus dans la zone de contrôle.

Fonctionnement du Contrôle de l'intégrité du système

1. **L'application intercepte les événements des opérations sur les fichiers**

   L'application utilise un mécanisme d'interception spécial qui dispose d'un accès en lecture seule au fichier en cours d'analyse.

2. **L'application vérifie si le fichier a été modifié.**

   Le Contrôle de l'intégrité du système suit les modifications apportées aux propriétés de fichier suivantes :

   - Contenu (`write ()`, `truncate ()` et autres modifications)
   - Métadonnées (modification des autorisations d'accès à l'aide des commandes `chmod` ou `chown`)
   - Horodatages (`utimensat`)
   - Attributs étendus (`setxattr`) et autres

3. **Fin de l'analyse**

   L'application génère un événement *Intégrité du système compromise* si le fichier a été modifié.

Configuration du Contrôle de l'intégrité du système

1. **Activer le Contrôle de l'intégrité du système**

   Par défaut, le contrôle de l'intégrité du système est désactivé. Sélectionnez les appareils sur lesquels vous souhaitez surveiller les modifications des fichiers en temps réel, puis activez le module Contrôle de l'intégrité du système sur ces appareils.

2. **Configurer la zone de contrôle**

   Pour que le module fonctionne, au moins une zone de contrôle doit être indiquée. Par défaut, la zone de contrôle des *Objets internes de Kaspersky* (`/opt/kaspersky/kesl/`) est définie.

   Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

   Configuration d'une zone de contrôle dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité → Contrôle de l'intégrité du système**.

5. Cliquez sur le lien **Zones de contrôle**.

   La fenêtre contenant le tableau des zones d'analyse s'ouvre.

6. Cliquez sur **Ajouter**.

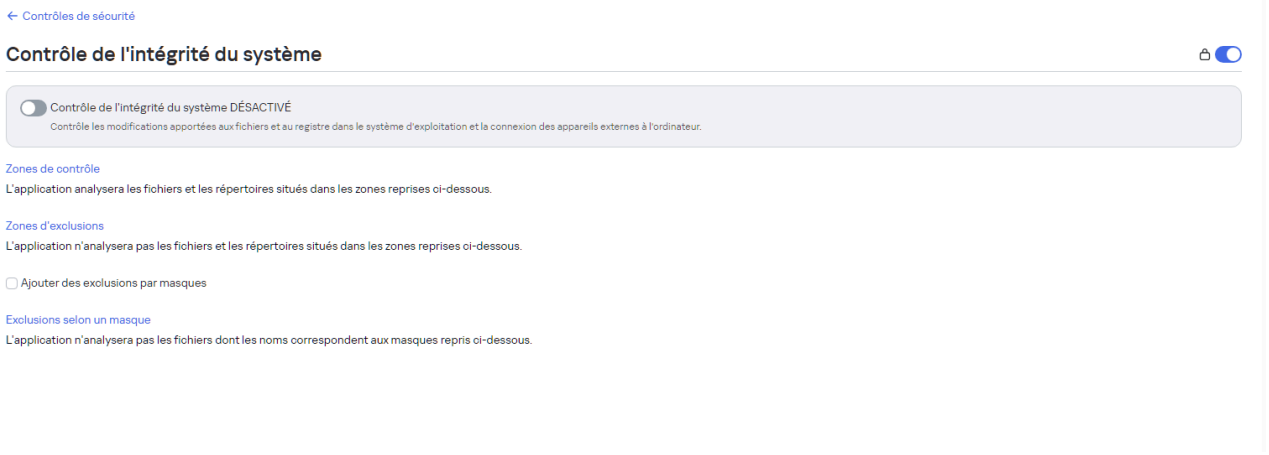
   La fenêtre d'ajout de zones d'analyse s'ouvre

7. Dans le champ **Nom**, indiquez le nom de la zone de contrôle, par exemple *Objets critiques*.

8. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

9. Si nécessaire, indiquez des masques pour les noms des objets au format de l'interpréteur de commandes (par exemple, `*.txt` ou `file?.*`). Ajoutez les masques un par un.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Contrôle de l'intégrité du système

Configuration d'une zone de contrôle via la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 11
```

Symboles

Options de la commande

Paramètre	Description
`UseScanArea=Yes`	Activation d'une zone de contrôle avec un ID `#`. Vous pouvez désactiver temporairement l'analyse d'une zone de contrôle au lieu de supprimer la zone. Pour ce faire, définissez `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Par exemple, `ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Chemin d'accès au répertoire à surveiller. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exemple

Une zone de contrôle qui inclut uniquement le répertoire `/etc` :

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3 Configurer des zones d'exclusion

Une exclusion a une priorité supérieure à celle d'une zone de contrôle. Un objet exclu n'est pas analysé, même s'il se trouve dans une zone de contrôle. Si une zone de surveillance est définie à un niveau inférieur au répertoire spécifié dans l'exclusion, l'application ne surveille pas cette zone de surveillance pendant la surveillance de l'intégrité du système.

Comment configurer une zone d'exclusion dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité → Contrôle de l'intégrité du système**.

Vous pouvez définir des exclusions d'après le chemin d'accès ou d'après le masque du nom de fichier. L'application peut exclure de l'analyse un répertoire entier (ou un fichier individuel) ou exclure des fichiers dont le nom correspond à un masque dans les zones de contrôle.

Pour ajouter des exclusions d'après le chemin d'accès :

1. Cliquez sur le lien **Zones d'exclusions**.

   Une fenêtre contenant un tableau des zones d'exclusion s'ouvre.
2. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'exclusion s'ouvre.
3. Dans le champ **Nom**, indiquez le nom de la zone d'exclusion, par exemple *Fichiers système*.

4. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

5. Spécifiez les masques de noms d'objets au format de l'interpréteur de commandes (par exemple `*.txt` ou `file?.*`). Ajoutez les masques un par un.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Pour ajouter des exclusions d'après le masque de nom de fichier :

1. Cochez la case **Ajouter des exclusions par masques**.

2. Cliquez sur le lien **Exclusions selon un masque**.

   Un tableau contenant les zones d'exclusion d'après le masque s'ouvre.

3. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'exclusion d'après le masque s'ouvre.

4. Spécifiez le masque du nom de fichier au format de l'interpréteur de commandes (par exemple, `*.txt` ou `file?.*`). Ajoutez les masques un par un.

5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer une zone d'exclusion sur la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 11
```

Symboles

Options de la commande

Paramètre	Description
`UseScanArea=Yes`	Exclut du contrôle la zone indiquée avec l'ID `#`. Vous pouvez désactiver temporairement une zone d'exclusion au lieu de la supprimer. Pour ce faire, définissez `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.
`AreaMask.item_#`	Restriction de la zone d'exclusion. Dans la zone d'exclusion, l'application exclut des analyses uniquement les objets indiqués à l'aide de masques au format de l'interpréteur de commandes. Par exemple, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Chemin d'accès au répertoire à exclure de l'analyse. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exemple

Une zone d'exclusion qui inclut uniquement le répertoire `/tmp` :

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

Vérification de l'intégrité du système

Lors de l'exécution de la tâche *Vérification de l'intégrité du système*, l'application compare l'état actuel de chaque objet à son état d'origine, ou état de référence. La référence contient les chemins vers les objets surveillés et leurs métadonnées. Cela permet de suivre les modifications des fichiers et répertoires inclus dans la zone de surveillance.

La référence peut contenir des données personnelles.

Contrairement au module Contrôle de l'intégrité du système, la tâche *Vérification de l'intégrité du système* aide à limiter le nombre d'événements et permet de générer un rapport récapitulatif sur les modifications du système d'exploitation.

Fonctionnement de la vérification de l'intégrité du système

1. **L'application prend un instantané du système**

   L'état de référence du système est créé lors de la première exécution de la tâche. Si vous avez créé plusieurs tâches de vérification de l'intégrité du système, un instantané du système distinct est créé pour chaque tâche. Pour les appareils Linux, l'état de référence est reconstruit lorsque les paramètres de la tâche changent, par exemple si une nouvelle zone de surveillance est ajoutée, ainsi que lorsque la tâche est lancée avec le paramètre **Actualiser l'instantané de l'état du système à chaque démarrage de la tâche** activé.

   Le stockage des états de référence se trouve dans `/var/opt/kaspersky/kesl/private/fim.db`. L'accès à une base de données contenant des références requiert des privilèges root. L'état de référence est supprimé avec la tâche de vérification de l'intégrité du système associée.

2. **L'application recherche les modifications de l'état du système**

   L'application applique les critères suivants pour comparer les informations sur les objets inclus dans la zone de surveillance :

   - Hachage SHA256 du fichier (pour une vérification complète)
   - heure de modification du fichier ;
   - Taille du fichier

3. **Fin de l'analyse**

   Si l'état actuel du système diffère de l'état de référence, Kaspersky Endpoint Security génère un événement de violation de l'intégrité du système : *Intégrité du système compromise*.

Configuration et exécution de la tâche de vérification de l'intégrité du système

1. **Créer une tâche de vérification de l'intégrité du système**

   Procédure de création de la tâche de vérification de l'intégrité du système dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
      La liste des tâches s'ouvre.
   2. Cliquez sur **Ajouter**.
      L'Assistant de création de tâche démarre.
   3. Configurez les paramètres de la tâche :
      a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux 12.5**.
      b. Dans la liste déroulante **Type de tâche**, choisissez **Vérification de l'intégrité du système**.
      c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Contrôle hebdomadaire de l'intégrité du système*.
      d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.
   4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche.
   5. Quittez l'Assistant.

   Procédure de création de la tâche de vérification de l'intégrité du système à partir de la ligne de commande

   Pour créer une tâche, exécutez la commande suivante :

   ```
   kesl-control --create-task <task name> --type ODFIM
   ```

   où `<task name>` est le nom de la nouvelle tâche.

   Cette commande renvoie l'ID de la tâche créée.

   Exemple de résultat de l'exécution de la commande :

   Tâche créée (ID de tâche : 115)

2. **Si nécessaire, modifiez les paramètres de la tâche**

   Configuration de la tâche de vérification de l'intégrité du système dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
      La liste des tâches s'ouvre.
   2. Cliquez sur la tâche Vérification de l'intégrité du système qui vient d'être créée.
      La fenêtre des propriétés de la tâche s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez le type d'analyse :

   - **Analyse complète**. L'application compare le hachage SHA256 du fichier dans son état actuel avec le hachage de l'instantané du système.

   - **Analyse rapide**. L'application compare uniquement les tailles des fichiers. Si la taille du fichier n'a pas changé, l'heure de modification n'est pas considérée comme un paramètre critique.

5. Dans la section **Paramètres de la Vérification de l'intégrité du système**, cochez les cases suivantes :

   - **Actualiser l'instantané de l'état du système à chaque démarrage de la tâche**. Si cette case est cochée, l'application recrée l'état de référence à chaque lancement de la tâche.

   - **Vérifier les répertoires dans les zones de surveillance**. Si cette case est cochée, l'application vérifie les répertoires indiqués par l'utilisateur. Si la case est décochée, l'application analyse uniquement la zone d'analyse par défaut – *Objets internes de Kaspersky* (`/opt/kaspersky/kesl/`).

   - **Suivre la dernière fois qu'un fichier a été consulté au début de chaque tâche**. Si cette case est cochée, l'application vérifie l'heure du dernier accès au fichier (le paramètre `noatime`) à chaque exécution de la tâche.

6. Enregistrez vos modifications.

Configuration de la tâche de vérification de l'intégrité du système à partir de la ligne de commande

Exécutez la commande :

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

Symboles

Paramètres de la tâche *Vérification de l'intégrité du système*

Paramètre	Description
`RebuildBaseline`	Recréer l'état de référence à chaque lancement de la tâche.
`CheckFileHash`	Analyse du hachage SHA256 du fichier. Si la vérification est désactivée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique).
`TrackDirectoryChanges`	Analyse des répertoires indiqués par l'utilisateur. Si le paramètre est désactivé, l'application analyse uniquement la zone par défaut (`/opt/kaspersky/kesl/`).
`TrackLastAccessTime`	Vérification de l'heure du dernier accès au fichier (paramètre `noatime`).
`UseExcludeMasks`	Exclusions du contrôle. Une nouvelle section `[ExcludeMasks.item_#]` sera ajoutée dans les paramètres de la tâche. L'application n'analysera pas les objets indiqués dans cette section. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.
`ExcludeMasks.item_#=<object mask>`	Exclusion d'objets de la zone de contrôle. Ce paramètre permet d'exclure un fichier individuel de la zone d'analyse spécifiée par son nom ou d'exclure plusieurs fichiers à la fois à l'aide de masques au format d'interpréteur de commandes. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. Ce paramètre peut être géré uniquement si le paramètre `UseExcludeMasks` est activé. Vous pouvez indiquer plusieurs masques. Chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index. Exemple : `ExcludeMasks.item_0000=<eicar1.*>`

3 Configurer la zone de contrôle

Il faut définir au moins une zone de contrôle pour que la tâche puisse démarrer. Par défaut, la zone de contrôle des *Objets internes de Kaspersky* (`/opt/kaspersky/kesl/`) est définie.

La tâche est exécutée uniquement si l'état de référence contient des informations sur les objets appartenant à la zone de contrôle de la tâche.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Configuration d'une zone de contrôle dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche Vérification de l'intégrité du système qui vient d'être créée.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Assurez-vous que la case **Vérifier les répertoires dans les zones de surveillance** est cochée.

5. Dans le groupe **Zone de surveillance et d'exclusion**, cliquez sur le lien **Zones de surveillance**.

   La fenêtre contenant le tableau des zones d'analyse s'ouvre.

6. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'analyse s'ouvre

7. Dans le champ **Nom**, saisissez un nom pour la zone de contrôle, par exemple *Fichiers sur le bureau*.

8. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

9. Le cas échéant, indiquez des masques pour les noms d'objets au format d'interpréteur de commandes (par exemple, `*.txt`, `file?.*`). Ajoutez les masques un par un.

10. Enregistrez vos modifications.

Configuration d'une zone de contrôle via la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les paramètres actuels, exécutez la commande suivante :

```
kesl-control --get-settings <task ID|name>
```

Symboles

Paramètres de la tâche *Vérification de l'intégrité du système*

Paramètre	Description
`UseScanArea=Yes`	Activation d'une zone de contrôle avec un ID `#`. Vous pouvez désactiver temporairement l'analyse d'une zone de contrôle au lieu de supprimer la zone. Pour ce faire, définissez `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `ScanScope.item_#.AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Par exemple, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Chemin d'accès au répertoire à surveiller. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exemple

Une zone de contrôle qui inclut uniquement le répertoire `/etc` :

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 Configurer des zones d'exclusion

Une exclusion a une priorité supérieure à celle d'une zone de contrôle. Un objet exclu n'est pas analysé, même s'il se trouve dans une zone de contrôle. Si une zone de surveillance est définie à un niveau inférieur au répertoire spécifié dans l'exclusion, l'application ne surveille pas cette zone de surveillance pendant la surveillance de l'intégrité du système.

Comment configurer une zone d'exclusion dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
2. La liste des tâches s'ouvre.
3. Cliquez sur la tâche Vérification de l'intégrité du système qui vient d'être créée.

   La fenêtre des propriétés de la tâche s'ouvre.
4. Sélectionnez l'onglet **Paramètres de l'application**.

Vous pouvez définir des exclusions d'après le chemin d'accès ou d'après le masque du nom de fichier. L'application peut exclure de l'analyse un répertoire entier (ou un fichier individuel) ou exclure des fichiers dont le nom correspond à un masque dans les zones de contrôle.

Pour ajouter des exclusions d'après le chemin d'accès :

1. Dans le groupe **Zone de surveillance et d'exclusion**, cliquez sur le lien **Zones d'exclusions**.

   Une fenêtre contenant un tableau des zones d'exclusion s'ouvre.
2. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'exclusion s'ouvre.
3. Dans le champ **Nom**, indiquez le nom de la zone d'exclusion, par exemple *Fichiers système*.

4. Dans le champ **Emplacement**, indiquez le chemin d'accès à un fichier particulier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

5. Spécifiez les masques de noms d'objets au format de l'interpréteur de commandes (par exemple `*.txt` ou `file?.*`). Ajoutez les masques un par un.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Pour ajouter des exclusions d'après le masque de nom de fichier :

1. Dans le groupe **Zone de surveillance et d'exclusion**, cliquez sur le lien **Exclusions selon un masque**.

   Un tableau contenant les zones d'exclusion d'après le masque s'ouvre.

2. Cliquez sur **Ajouter**.

   La fenêtre d'ajout de zones d'exclusion d'après le masque s'ouvre.

3. Spécifiez le masque du nom de fichier au format de l'interpréteur de commandes (par exemple, `*.txt` ou `file?.*`). Ajoutez les masques un par un.

4. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer une zone d'exclusion sur la ligne de commande

1. Exécutez la commande suivante :

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Pour vérifier les paramètres actuels, exécutez la commande suivante :

```
kesl-control --get-settings <task ID|name>
```

Symboles

Paramètres de la tâche *Vérification de l'intégrité du système*

Paramètre	Description
`UseScanArea=Yes`	Exclut du contrôle la zone indiquée avec l'ID `#`. Vous pouvez désactiver temporairement une zone d'exclusion au lieu de la supprimer. Pour ce faire, définissez `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.
`AreaMask.item_#`	Restriction de la zone d'exclusion. Dans la zone d'exclusion, l'application exclut des analyses uniquement les objets indiqués à l'aide de masques au format de l'interpréteur de commandes. Vous pouvez définir plusieurs éléments `ExcludedFromScanScope.item_#.AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Par exemple, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Chemin d'accès au répertoire à exclure de l'analyse. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exemple

Une zone d'exclusion qui inclut uniquement le répertoire `/tmp` :

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5. **Lancement de la tâche**

Lancement de la tâche de vérification de l'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cochez la case en regard de la tâche créée.

3. Cliquez sur **Démarrer**.

Lancement de la tâche de vérification de l'intégrité du système sur la ligne de commande

Pour lancer la tâche, exécutez la commande suivante :

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `[-W]` : activer la sortie des événements actuels liés à cette tâche.
- `[--progress]` : activer l'affichage de la progression de la tâche.

Exclusions de l'analyse pour l'application

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas.

L'administrateur du système forme indépendamment la zone de confiance, en tenant compte des propriétés des objets gérés et des applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Paramètres	Description
Adresses Internet	Adresses Internet que le module Protection contre les menaces Internet considère comme fiables. Le module n'analyse pas le trafic entrant et sortant de ces adresses à la recherche de menaces. La liste des adresses de confiance peut être utilisée, par exemple, si le module empêche le téléchargement d'un fichier à partir d'un site connu. Pour plus d'informations, consultez l'article Comment ajouter des adresses Internet de confiance
Adresses IP	Adresses IP des appareils de confiance. Le module Protection contre les menaces réseau ne bloque pas l'activité réseau provenant de ces adresses. L'application n'ajoute pas non plus au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions. Pour plus d'informations, consultez l'article Comment ajouter une adresse IP de confiance d'un ordinateur
Ports réseau	La liste des ports réseau que le module Protection contre les menaces réseau exclut de l'analyse. Pour plus d'informations, consultez l'article Comment sélectionner les ports réseau surveillés
Certificats racine	Certificats racines que Kaspersky Endpoint Security considère comme étant de confiance. La liste des certificats racines de confiance est utilisée lorsque les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet analysent les connexions chiffrées (connexions HTTPS). Pour plus d'informations, consultez l'article Comment ajouter un certificat à la liste des certificats racines de confiance
Domaines	Liste des domaines de confiance. Les modules Protection contre les menaces Internet et Contrôle Internet ne contrôlent pas les connexions chiffrées avec ces domaines. Pour plus d'informations, consultez l'article Comment ajouter un domaine de confiance
Points de montage	Liste des points de montage fiables. Les modules Protection contre les fichiers malicieux, Protection contre le chiffrement et Analyse du conteneur excluent de l'analyse les points de montage spécifiés. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`. Pour plus d'informations, consultez l'article Comment exclure des points de montage
Applications	Applications pour lesquelles Kaspersky Endpoint Security ne contrôle ni l'activité liée aux fichiers et au réseau ni l'accès au registre système. Les modules de protection tels que Protection contre les fichiers malicieux ou Détection comportementale ne contrôlent pas l'activité des applications spécifiées. Pour plus d'informations, consultez l'article Comment ajouter des applications de confiance
Exclusions de l'analyse des logiciels malveillants	Fichiers ou dossiers, ainsi que types d'objets (selon l'Encyclopédie des virus), exclus de l'analyse par tous les modules de l'application ou certains d'entre eux. Pour plus d'informations, consultez l'article Comment ajouter des exclusions de la protection
Appareils	Appareils auxquels le module Contrôle des appareils accorde toujours un accès complet aux utilisateurs ou groupes sélectionnés. Pour plus d'informations, consultez l'article Comment ajouter des appareils de confiance

Comment ajouter des exclusions de la protection

Une *exclusion de la protection* est un ensemble de conditions qui doivent être remplies pour que l'application Kaspersky Endpoint Security ne recherche pas de virus et autres applications malveillantes dans les objets.

Vous pouvez ajouter des exclusions de protection de différentes manières :

- **Exclusions par chemin d'accès**. Chemin d'accès à un fichier ou à un répertoire, ou masque de chemin d'accès. Le chemin d'accès à un répertoire doit se terminer par une barre oblique `/`.

  Pour spécifier des chemins dans des conteneurs ou des images, utilisez des tags.

  Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

- **Exclusions par masque**. Masque de nom d'objet. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis.
- **Exclusions par nom de menace** Nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Vous pouvez indiquer un nom de menace à l'aide d'un masque.
- **Exclusions par processus** Chemin d'accès à un processus ou masque de chemin d'accès à un processus. Le chemin d'accès à un répertoire doit se terminer par une barre oblique `/`.

Kaspersky Endpoint Security permet également d'exclure les fichiers de certains formats : les archives, les bases de données de messagerie, les fichiers texte et les fichiers journaux de base de données.

Comment définir des masques dans les exclusions par chemin d'accès

L'application prend en charge les masques pour définir des exclusions d'analyse en fonction du chemin d'accès à un fichier, à un répertoire ou à un processus :

- Le caractère `*` (astérisque) remplace n'importe quelle suite de caractères, à l'exception des caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/*/*.txt` inclut tous les chemins d'accès aux fichiers portant l'extension TXT situés dans des répertoires du répertoire `dir`, mais pas dans leurs sous-répertoires.

- Les caractères `**` remplacent n'importe quelle suite de caractères (y compris une suite vide) dans un nom de fichier ou de répertoire, y compris les caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/**/*.txt` inclut tous les chemins d'accès aux fichiers portant l'extension TXT situés dans des répertoires imbriqués dans le répertoire `dir`, à l'exclusion du répertoire `dir` lui-même.

- Le caractère `?` (point d'interrogation) remplace n'importe quel caractère unique, à l'exception des caractères `\` et `/` (séparateurs des noms de fichiers et de répertoires dans les chemins d'accès aux fichiers et aux répertoires). Par exemple, le masque `/dir/???.txt` inclut les chemins d'accès à tous les fichiers situés dans le répertoire nommé `dir` qui portent l'extension TXT et dont le nom comporte trois caractères.

Kaspersky Endpoint Security peut traiter différemment les exclusions définies à l'aide de masques selon le mécanisme d'interception des événements système sélectionné (module de noyau mis à jour ou technologie fanotify). Le tableau ci-dessous présente un exemple de traitement des exclusions définies à l'aide de masques pour la technologie fanotify et le module de noyau mis à jour. Pour en savoir plus sur le traitement des exclusions pour le module de noyau mis à jour, consultez le tableau *Différences entre les exclusions définies à l'aide de masques pour le module de noyau mis à jour*.

Exemple d'exclusions définies à l'aide de masques pour la technologie fanotify et le module de noyau mis à jour

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home Ce masque de chemin exclura tous les objets du répertoire /home et de ses sous-répertoires. La stratégie peut être appliquée à différents appareils : sur l'un, eicar est un nom de répertoire, tandis que sur un autre, il s'agit d'un nom de fichier. Dans ce cas, le fichier nommé eicar et le répertoire seront tous deux exclus de l'analyse.	/home/ ├── eicar – **Exclus** ├── eicar.txt – **Exclus** ├── eicar.file – **Exclus** └── test1/ – **Exclus** │ ├── eicar – **Exclus** │ ├── eicar.txt – **Exclus** │ ├── eicar.file – **Exclus** │ └── level1/ – **Exclus** │ │ ├── eicar – **Exclus** │ │ ├── eicar.txt – **Exclus** │ │ ├── eicar.file – **Exclus** │ │ └── level2/ – **Exclus** /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/ Ce masque de chemin exclura tous les objets du répertoire /home et de ses sous-répertoires.	

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/* Ce masque de chemin exclura tous les objets du répertoire /home et de ses sous-répertoires.	

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*.txt Ce masque de chemin d'accès exclut les fichiers portant l'extension TXT du répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – **Exclus** ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*.* Ce masque de chemin d'accès exclut les fichiers de tout format du répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – **Exclus** ├── eicar.file – **Exclus** └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**.txt Ce modèle de chemin d'accès exclura les fichiers portant l'extension TXT du répertoire /home et de ses sous-répertoires.	/home/ ├── eicar – Analysé ├── eicar.txt – **Exclus** ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – **Exclus** │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – **Exclus** │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**.* Ce modèle de chemin d'accès exclura les fichiers de tout format du répertoire /home et de ses sous-répertoires.	/home/ ├── eicar – Analysé ├── eicar.txt – **Exclus** ├── eicar.file – **Exclus** └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – **Exclus** │ ├── eicar.file – **Exclus** │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – **Exclus** │ │ ├── eicar.file – **Exclus** │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/*.txt Ce masque de chemin exclura les fichiers portant l'extension .TXT situés dans le répertoire de premier niveau par rapport au répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – **Exclus** │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/*.* Ce masque de chemin exclura les fichiers de tous formats situés dans le répertoire de premier niveau par rapport au répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – **Exclus** │ ├── eicar.file – **Exclus** │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**/*.txt Ce masque de chemin exclura les fichiers portant l'extension TXT dans le répertoire /home ; l'application analysera les fichiers TXT situés directement dans le répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – **Exclus** │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – **Exclus** │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/* ou /home/**/* Ce masque de chemin exclura les fichiers de tous formats, y compris ceux sans extension, dans les sous-répertoires de /home ; l'application analysera les fichiers situés directement dans le répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ │ ├── eicar – **Exclus** │ ├── eicar.txt – **Exclus** │ ├── eicar.file – **Exclus** │ └── level1/ – Analysé │ │ ├── eicar – **Exclus** │ │ ├── eicar.txt – **Exclus** │ │ ├── eicar.file – **Exclus** │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/eicar Ce masque de chemin exclura les fichiers sans extension nommés eicar dans le répertoire /home.	/home/ ├── eicar – **Exclus** ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/eicar Ce masque de chemin exclut les fichiers sans extension portant le nom eicar dans le répertoire de premier niveau par rapport au répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – **Exclus** │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**/eicar Ce masque de chemin exclura les fichiers sans extension nommés eicar situés dans les sous-répertoires de /home ; l'application analysera les fichiers situés directement dans le répertoire /home.	/home/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – **Exclus** │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – **Exclus** │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Pour un module de noyau mis à jour, les exclusions définies à l'aide de masques peuvent fonctionner différemment. Le tableau ci-dessous présente uniquement les différences concernant les exclusions définies à l'aide de masques de chemin par rapport à la technologie fanotify.

Différences concernant les exclusions définies à l'aide de masques pour un module de noyau mis à jour

Structure	Exclusion	Résultat
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/* Ce masque de chemin exclura tous les objets du répertoire /home et de ses sous-répertoires.	/home/ ├── eicar – **Exclus** ├── eicar.txt – **Exclus** ├── eicar.file – **Exclus** └── test1/ – Analysé │ ├── eicar – **Exclus** │ ├── eicar.txt – **Exclus** │ ├── eicar.file – **Exclus** │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ ├── eicar.file – Analysé │ │ └── level2/ – Analysé /home2/ ├── eicar – Analysé ├── eicar.txt – Analysé ├── eicar.file – Analysé └── test1/ – Analysé │ ├── eicar – Analysé │ ├── eicar.txt – Analysé │ ├── eicar.file – Analysé │ └── level1/ – Analysé │ │ ├── eicar – Analysé │ │ ├── eicar.txt – Analysé │ │ └── eicar.file – Analysé

Comment ajouter des exclusions de la protection

Comment ajouter des exclusions de protection dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Cliquez sur le lien **Exclusions de l'analyse**.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

7. Cochez les cases correspondant aux critères que vous souhaitez utiliser pour une exclusion de protection :

   - **Chemin d'accès au fichier ou au dossier**. Spécifiez un chemin d'accès à un fichier ou à un répertoire, ou un masque de nom de fichier. Pour spécifier des chemins dans des conteneurs ou des images, utilisez des tags.

     Pour un système de fichiers local, indiquez le chemin d'accès à un répertoire (par exemple, `/path/to/folder/`). Pour un système de fichiers monté ou tous les systèmes de fichiers montés à distance, saisissez un masque de nom de fichier. Pour un système de fichiers monté, spécifiez également le protocole d'accès (NFS, Samba ou personnalisé).

   - **Type d'objet**. Spécifiez le nom de la menace.

   - **Hachage de l'objet**. Saisissez le hachage SHA256 de l'objet. Vous pouvez également ajouter un fichier ou spécifier un événement à partir duquel dériver le hachage SHA256 pour l'exclusion.

8. Sélectionnez les modules de protection auxquels vous souhaitez appliquer l'exclusion :

   - **Tous les modules de la protection**. L'exclusion s'applique à tous les modules de protection concernés par **Exclusions de l'analyse des logiciels malveillants**.

   - **Modules de protection sélectionnés**. Sélectionnez les modules auxquels vous souhaitez appliquer l'exclusion : Protection contre les fichiers malicieux, Protection contre le chiffrement, Protection contre les Exploits.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter des exclusions de protection en ligne de commande

1. Pour ajouter une exclusion par chemin d'accès, exécutez la commande suivante :

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. Pour ajouter une exclusion par masque, procédez comme suit :

   a. Activez l'exclusion de fichiers par masque :

```
kesl-control --set-settings 1 UseExcludeMasks=Yes
```

   b. Ajoutez un masque de nom de fichier :

```
kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
```

3. Pour ajouter une exclusion par nom de menace, procédez comme suit :

   a. Activez l'exclusion de fichiers par nom de menace :

```
kesl-control --set-settings 1 UseExcludeThreats=Yes
```

   b. Ajoutez un nom de menace :

```
kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
```

4. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 1
```

Symboles

Options de la commande

Paramètre	Description
`--add-exclusion`	Exclure un répertoire de l'analyse. Une nouvelle section `[ExcludedFromScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application exclura des analyses les objets du répertoire spécifié par le paramètre `path`.
`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Utilisez des masques au format shell pour saisir le nom du fichier. Exemple : `ExcludeMasks.item_0000=*_my_file_??.html`.
`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet. Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse. Exemple : `ExcludeThreats.item_0000=EICAR-Test-*`.

Comment ajouter des exclusions de protection dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre **Propriétés : <Policy name>** s'ouvre.
3. Passez à la section **Protection principale** → **Exclusions de la Protection contre les fichiers malicieux**.

Pour ajouter des exclusions d'après le chemin d'accès :

1. Sous **Exclusions**, cliquez sur **Configurer**.

   Une fenêtre contenant un tableau des zones d'exclusion s'ouvre.
2. Cliquez sur **Ajouter**.
3. Indiquez le nom de la zone d'exclusion, par exemple *Fichiers système*.
4. Indiquez le chemin d'accès à un fichier ou à un répertoire (par exemple `/path/to/folder`). Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
5. Spécifiez les masques de noms d'objets au format de l'interpréteur de commandes (par exemple `*.txt` ou `file?.*`). Ajoutez les masques un par un.
6. Enregistrez vos modifications.

Pour ajouter des exclusions d'après le masque de nom de fichier :

1. Sous **Exclusions d'après le masque**, cliquez sur le bouton **Configurer**.

   Une fenêtre contenant un tableau des zones d'exclusion par masque s'ouvre.
2. Cliquez sur **Ajouter**.

3. Spécifiez le masque du nom de fichier au format de l'interpréteur de commandes (par exemple, `*.txt` ou `file?.*`). Ajoutez les masques un par un.

4. Enregistrez vos modifications.

Pour ajouter des exclusions par nom de menace :

1. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions d'après le nom de la menace**.

   Une fenêtre contenant un tableau des zones d'exclusion par nom de menace s'ouvre.

2. Cliquez sur **Ajouter**.

3. Spécifiez le nom de la menace. Nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Vous pouvez indiquer un nom de menace à l'aide d'un masque.

4. Enregistrez vos modifications.

Pour ajouter des exclusions par processus :

1. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions par processus**.

   Une fenêtre contenant un tableau des zones d'exclusion par processus s'ouvre.

2. Cliquez sur **Ajouter**.

   La fenêtre **Processus de confiance** s'ouvre.

3. Indiquez le nom de la zone d'exclusion.

4. Indiquez le chemin d'accès complet au processus exclu.

5. Le cas échéant, cochez la case **Appliquer aux processus enfants**. L'application exclut de l'analyse les processus enfants du processus exclu.

6. Cochez la case **Utiliser cette zone**. L'application exclut cette zone de l'analyse. La case est cochée par défaut.

7. Sous **Chemin d'accès aux fichiers modifiés**, sélectionnez le type de système de fichiers dans lequel se trouvent les répertoires à exclure des analyses :

   - **Local** pour les répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local.
   - **Monté** pour les répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers.
   - **Partagé** pour les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS.
   - **Tous les systèmes montés distants** pour tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
   - **Tous les systèmes partagés** pour toutes les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.

8. Spécifiez les masques de noms d'objets au format de l'interpréteur de commandes (par exemple `*.txt` ou `file?.*`). Ajoutez les masques un par un.

9. Enregistrez vos modifications.

Comment ajouter des adresses Internet de confiance

Outre les sites Internet malveillants et de phishing, la Protection contre les menaces Internet peut bloquer d'autres sites Internet. Par exemple, la Protection contre les menaces Internet bloque le trafic HTTP qui ne répond pas aux normes RFC. Vous pouvez composer une liste des URL dont vous faites confiance au contenu. Le module Protection contre les menaces Internet ne recherche pas la présence éventuelle de virus et d'autres applications présentant une menace dans les informations en provenance des adresses Internet de confiance. Cette fonctionnalité peut être utilisée, par exemple, si le module Protection contre les menaces Internet empêche le téléchargement d'un fichier depuis un site Internet que vous connaissez.

Ajout d'une adresse Internet de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Adresses Internet**.
   Une fenêtre contenant la liste des adresses Internet de confiance s'ouvre.
6. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable.
   Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
   Vous pouvez également importer une liste d'adresses Internet de confiance à partir d'un fichier JSON.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Ajout d'une adresse Internet de confiance via la ligne de commande

1. Pour activer la liste des adresses Internet de confiance, exécutez la commande suivante :

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. Pour ajouter une adresse Internet de confiance, exécutez la commande suivante :

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. Pour vérifier les valeurs actuelles des paramètres du module, exécutez la commande suivante :

```
kesl-control --get-settings 14
```

Exemple

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

Comment ajouter l'adresse IP de confiance d'un ordinateur

Kaspersky Endpoint Security peut reconnaitre une attaque réseau et bloquer une connexion réseau non sécurisée qui transmet un grand nombre de paquets (par exemple, provenant de caméras de surveillance). Pour travailler avec des appareils de confiance, vous pouvez ajouter les adresses IP de ces appareils à la liste des exclusions. Les adresses Internet de confiance affectent le module Protection contre les menaces réseau.

Configuration des adresses exclues du blocage dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Adresses IP**.
   Une fenêtre contenant la liste des adresses IP de confiance s'ouvre.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
7. Saisissez l'adresse IP de l'ordinateur à l'origine des attaques réseaux qui ne devront pas être bloquées.
   Le cas échéant, indiquez le sous-réseau.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration des adresses exclues du blocage via la ligne de commande

1. Pour appliquer les adresses IP de confiance, exécutez la commande suivante :

   ```
   kesl-control --set-settings 17 UseExcludeIPs=Yes
   ```

2. Pour ajouter une adresse IP de confiance, exécutez la commande suivante :

   ```
   kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
   ```

3. Pour analyser la liste des adresses IP de confiance, exécutez la commande suivante :

   ```
   kesl-control --get-settings 17 TrustedIPAddresses
   ```

Exemple

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

Comment sélectionner les ports réseau surveillés

Kaspersky Endpoint Security surveille les flux de données transmis via certains protocoles et qui transitent par certains ports TCP ouverts sur l'ordinateur de l'utilisateur. Par défaut, l'application contrôle les ports connus et enregistrés, par exemple le port 443 pour les connexions HTTPS et le port 143 pour le protocole de messagerie IMAP.

Les *ports réseau de confiance* sont des ports réseau que le module Protection contre les menaces réseau exclut de l'analyse. Cette opération est nécessaire pour configurer Kaspersky Endpoint Security afin d'assurer la compatibilité avec des services et applications tiers de confiance, ainsi que pour optimiser les performances. Par exemple, vous pouvez spécifier des ports réseau pour les services de sauvegarde internes afin que l'application n'interfère pas avec le téléchargement ou l'envoi des copies de sauvegarde.

Il est important de garder à l'esprit que l'exclusion des ports réseau de l'analyse rend l'appareil moins protégé. Essayez de limiter les exclusions au minimum.

Comment exclure les ports réseau de l'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance** → **Ports réseau**.

   Cette action ouvre une fenêtre contenant la liste des ports réseau surveillés.
5. Désactivez le commutateur pour les ports que vous souhaitez exclure de l'analyse.

   Si le port dont vous avez besoin ne figure pas dans la liste, cela signifie que l'application n'analyse pas ce port.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exclure les ports réseau de l'analyse dans la ligne de commande

1. Obtenez la liste des ports surveillés en exécutant la commande suivante :

   ```
   kesl-control --get-net-setting
   ```
2. Si la surveillance de tous les ports est activée (`MonitorNetworkPorts=All`), exécutez la commande suivante :

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=Selected
   ```

   Cela ajoute une section `[NetworkPorts.item_#]` contenant les ports réseau surveillés.

3. Si la section contient un port que vous souhaitez exclure de l'analyse, procédez comme suit :

   a. Pour écrire les paramètres d'analyse du trafic réseau dans un fichier, exécutez la commande suivante :

   ```
   kesl-control --get-net-setting --file <path to file>
   ```

   b. Dans ce fichier, supprimez les sections `[NetworkPorts.item_#]` contenant les ports réseau que vous ne souhaitez pas surveiller.

   c. Pour appliquer vos paramètres, exécutez la commande suivante :

   ```
   kesl-control --set-net-settings --file <path to file>
   ```

   Les paramètres modifiés sont importés dans l'application.

Comment ajouter un certificat à la liste des certificats racines de confiance

Kaspersky Endpoint Security vous permet d'installer des certificats racine de confiance sur les ordinateurs des utilisateurs si, par exemple, vous devez déployer un nouveau centre de certification. L'application vous permet d'ajouter un certificat à une liste de certificats spéciale de Kaspersky Endpoint Security. Dans ce cas, le certificat est considéré comme étant fiable uniquement pour l'application Kaspersky Endpoint Security. Autrement dit, l'utilisateur peut accéder à un site Internet avec le nouveau certificat dans le navigateur. Si une autre application tente d'accéder au site Internet, vous pouvez obtenir une erreur de connexion en raison d'un problème de certificat.

Les certificats racines de confiance sont utilisés par les modules suivants :

- Protection contre les menaces Internet
- Protection contre les menaces par emails
- Contrôle Internet

Les certificats de confiance aux formats CER, CRT, PEM et DER sont pris en charge. La taille maximale du fichier d'un certificat de confiance est de 2 Mo.

Comment installer un certificat racine de confiance dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance** → **Certificats racine**.
   Une fenêtre contenant la liste des certificats racines de confiance s'ouvre.
5. Cliquez sur **Ajouter**.
   Le formulaire d'ajout d'un certificat s'ouvre.

6. Chargez le certificat.
7. Si nécessaire, saisissez une description du certificat dans le champ **Commentaires**.
8. Enregistrez vos modifications.

Dans la liste des certificats de confiance, le numéro de série est utilisé comme nom du certificat.

Comment installer un certificat racine de confiance sur la ligne de commande

1. Pour ajouter un certificat, exécutez la commande suivante :

```
kesl-control --add-certificate <path to certificate>
```

2. Pour consulter la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --list-certificates
```

Les informations suivantes sont affichées pour chaque certificat :

- Objet du certificat
- numéro de série du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- empreinte digitale du certificat SHA256.

3. Pour supprimer un certificat de la liste, exécutez la commande suivante :

```
kesl-control --remove-certificate <certificate subject>
```

Comment ajouter un domaine de confiance

Kaspersky Endpoint Security dispose d'une liste de domaines de confiance pour lesquels il n'analyse pas les connexions chiffrées. Les domaines de confiance ont une incidence sur Protection contre les menaces Internet et Contrôle Internet. L'exclusion de domaines de l'analyse vous permet d'éviter de bloquer le trafic provenant de sources que vous connaissez.

Indiquez le nom de domaine. Les adresses Internet, telles que `example.com/*` ou `https://example.com`, sont ignorées.

Comment spécifier des domaines de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance** → **Domaines de confiance**.
   Une fenêtre contenant la liste des domaines de confiance s'ouvre.
5. Cliquez sur **Ajouter**.
   Le formulaire d'ajout d'un domaine s'ouvre.
6. Spécifiez un nom de domaine ou un masque de domaine. Par exemple, `*example.com`.
7. Enregistrez vos modifications.

Comment spécifier des domaines de confiance sur la ligne de commande

1. Pour ajouter un domaine, exécutez la commande suivante :

   ```
   kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
   ```

2. Pour tester vos paramètres, exécutez la commande suivante :

   ```
   kesl-control --get-net-settings
   ```

   Les domaines de confiance doivent être répertoriés dans la section `[Exclusions.item_#]`.

Exemple

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

Comment exclure des points de montage

Pour exclure les fichiers d'un répertoire particulier non seulement de l'analyse, mais également de l'interception, vous devez exclure le point de montage dans son ensemble. Ces exclusions sont appelées *exclusions globales*. L'application exclut de l'analyse et de l'interception des opérations sur les fichiers les répertoires locaux ou distants de confiance montés sur l'appareil. Par exemple, vous pouvez exclure les points de montage qui contiennent des fichiers temporaires afin de réduire la charge sur le système et d'accélérer la fin des analyses.

Les exclusions de points de montage ont une incidence sur les modules suivants :

- Protection contre les fichiers malicieux
- Protection contre le chiffrement
- Analyse du conteneur

Les points de montage de confiance sont également exclus de l'analyse par les tâches suivantes :

- Analyse des logiciels malveillants ;
- Analyse des zones critiques.
- Analyse du conteneur
- Analyse des disques amovibles.

Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.

Comment spécifier des points de montage de confiance dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance** → **Points de montage**.
   Une fenêtre contenant la liste des points de montage de confiance s'ouvre.
5. Cliquez sur **Ajouter**.
   Le formulaire d'ajout d'un point de montage s'ouvre.
6. Dans la liste déroulante des systèmes de fichiers, sélectionnez le type de système de fichiers sur lequel se trouvent les répertoires à exclure : **Local**, **Monté**, **Tous les systèmes montés distants**.
   Kaspersky Endpoint Security prend en charge les protocoles Samba et NFS pour les répertoires distants.

   Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.
7. Saisissez le nom du système de fichiers qui contient les répertoires à exclure.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment spécifier des points de montage de confiance dans la ligne de commande

1. Si le répertoire n'est pas un point de montage, transformez-le en point de montage en exécutant la commande suivante :

   ```
   mount --bind <path to dir> <path to dir>
   ```
2. Pour conserver le point de montage après le redémarrage du serveur, ajoutez la ligne suivante au fichier `/etc/fstab` :

   ```
   <path to dir> <path to dir> none defaults,bind 0 0
   ```

3. Redémarrez Kaspersky Endpoint Security :

```
systemctl restart kesl
```

4. Pour ajouter un point de montage de confiance, exécutez la commande suivante :

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. Redémarrez l'application pour appliquer les exclusions globales :

```
systemctl restart kesl
```

Exemple

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

Comment ajouter des applications de confiance

La *liste des applications de confiance* est une liste d'applications pour lesquelles Kaspersky Endpoint Security ne surveille pas l'activité des fichiers et des processus (y compris l'activité malveillante) ni la mémoire des processus. Par défaut, Kaspersky Endpoint Security surveille les objets ouverts, exécutés ou enregistrés par n'importe quel processus d'application et contrôle l'activité de toutes les applications.

Les applications de confiance affectent les modules suivants :

- Protection contre les fichiers malicieux
- Détection comportementale

Ainsi que les exclusions de l'analyse de la mémoire des processus.

Comment spécifier des applications de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance** → **Applications de confiance**.
   Une fenêtre reprenant la liste des applications de confiance s'ouvre.

5. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'applications de confiance pour tous les ordinateurs de l'organisation. Les listes des applications de confiance des stratégies parent et enfant sont fusionnées. Les applications de la stratégie parent s'affichent dans les stratégies enfant uniquement à des fins de consultation ; elles ne peuvent pas être modifiées ni supprimées.

   La fusion des listes est possible si vous avez activé l'héritage des paramètres de la stratégie parent.

6. Cliquez sur **Ajouter**.

   Le formulaire d'ajout d'une application s'ouvre.

7. Spécifiez le chemin d'accès à l'application ou un masque de chemin d'accès.

8. Configurez les paramètres de l'application de confiance :

   - **Ne pas analyser les fichiers ouverts par cette application**. Tous les fichiers qui sont ouverts par l'application sont exclus des analyses par Kaspersky Endpoint Security.
   - **Ne pas surveiller l'activité de l'application**. Kaspersky Endpoint Security ne surveille pas l'activité des fichiers et du réseau d'une application de confiance au sein du système d'exploitation.

     Vous pouvez également configurer la surveillance de l'activité des applications séparément pour les modules MDR et EDR (KATA) en cochant la case **Ne pas surveiller pour Managed Detection and Response et Endpoint Detection and Response**.
   - **Ne pas surveiller l'activité des applications enfants**. Kaspersky Endpoint Security ne surveille pas l'activité des fichiers et du réseau des applications lancées par une application de confiance.
   - **Ne pas analyser la mémoire de l'application en question**. Kaspersky Endpoint Security n'analyse pas la mémoire des processus générés par une application de confiance.

   Dans Web Console, le paramètre **Commentaires** n'est pas disponible pour Kaspersky Endpoint Security for Linux.

9. Enregistrez vos modifications.

Comment spécifier des applications de confiance dans la ligne de commande

1. Pour exclure de l'analyse l'activité des fichiers d'une application de confiance, exécutez la commande suivante :

   ```
   kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
   ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
   [ExcludedForProgram.item_#.ApplyToDescendants=Yes]
   ```

2. Pour exclure de l'analyse l'activité des processus d'une application de confiance, exécutez la commande suivante :

   ```
   kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
   TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
   [TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
   ```

3. Pour exclure de l'analyse la mémoire des processus d'une application de confiance, exécutez la commande suivante :

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

Symboles

Options de la commande

Paramètre	Description
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	Exclut de l'analyse par le module Protection contre les fichiers malicieux l'activité des fichiers d'une application de confiance.
`ExcludedForProgram.item_#.ProgramPath`	Chemin d'accès à l'application de confiance avec l'ID `#`. Le module Protection contre les fichiers malicieux n'analyse pas les processus de l'application indiquée. Si un module de noyau mis à jour est utilisé pour intercepter les événements système, le processus spécifié est exclu de l'interception dans tous les espaces de noms.
`ExcludedForProgram.item_#.AreaDesc`	Nom de l'application de confiance avec l'ID `#`.
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	Exclut de l'analyse par le module Protection contre les fichiers malicieux les processus enfants d'une application de confiance.
`UseTrustedPrograms=Yes`	Exclut de l'analyse par le module Détection comportementale l'activité des processus des applications de confiance.
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	Exclut de l'analyse l'activité d'une application de confiance avec l'ID `#`.
`TrustedPrograms.item_#.ProgramPath`	Chemin d'accès à l'application de confiance avec l'ID `#`. Le module Détection comportementale n'analyse pas les processus de l'application indiquée. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
`TrustedPrograms.item_#.ProgramDesc`	Nom de l'application de confiance avec l'ID `#`.
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	Exclut de la collecte de télémétrie par les modules Managed Detection and Response et Endpoint Detection and Response Expert (on-premises) l'activité d'une application de confiance.
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	Exclut de l'analyse par le module Détection comportementale les processus enfants d'une application de confiance.
`MemScanExcludedProgramPath.item_#`	Chemin d'accès à l'application de confiance avec l'ID `#`. L'application n'analyse pas la mémoire des processus de l'application de confiance.

Comment ajouter des appareils de confiance

Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Pour pouvoir utiliser les appareils de confiance, vous pouvez accorder l'accès à un utilisateur individuel, à un groupe d'utilisateurs ou à tous les utilisateurs de l'organisation. Par exemple, si votre organisation n'autorise pas l'utilisation de disques amovibles, mais que les administrateurs utilisent de tels disques dans le cadre de leur travail, vous pouvez autoriser l'utilisation des disques amovibles uniquement pour le groupe d'administrateurs. Pour ce faire, ajoutez un disque amovible à la liste de confiance et configurez les privilèges d'accès des utilisateurs.

Vous pouvez ajouter des appareils de confiance en fonction des données suivantes :

- **Identifiant**. Chaque appareil possède un identifiant unique (Hardware ID ou HWID). Vous pouvez consulter l'identificateur dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Exemple d'identifiant d'appareil : `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'ajout d'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers.

- **Par masque d'identifiant**. Si vous utilisez plusieurs appareils avec des identifiants similaires, vous pouvez ajouter des appareils à la liste de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Le caractère `?` remplace n'importe quel caractère unique. Par exemple, `WDC_C*`.

Comment ajouter des appareils de confiance dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôle des appareils** → **Appareils de confiance**.

   Une fenêtre contenant une liste des appareils de confiance s'ouvre.

5. Cliquez sur **Ajouter**.

   Le formulaire d'ajout d'un appareil s'ouvre.

6. Sous **Utilisateur ou groupe**, indiquez un utilisateur ou un groupe d'utilisateurs pour lequel l'appareil sera considéré comme un appareil de confiance.

   Vous pouvez sélectionner des utilisateurs dans la liste des comptes de Kaspersky Security Center ou en saisissant manuellement un nom d'utilisateur local. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   Par défaut, l'accès aux appareils de confiance est autorisé pour le groupe Tous.

7. Sous **Type d'appareil**, sélectionnez un type d'appareil dans la liste déroulante (par exemple, **Disques amovibles**).

8. Si vous souhaitez ajouter un appareil à partir d'un masque d'identifiant, cochez la case **Utiliser un masque**.

9. Dans le champ **Rechercher des appareils de confiance**, saisissez un identifiant d'appareil ou un masque d'identifiant.

   Le tableau affiche la liste des appareils qui répondent aux critères définis.

10. Cochez les cases en regard des noms des appareils que vous souhaitez ajouter à la liste des appareils de confiance.

11. Le cas échéant, décrivez, dans l'onglet **Commentaires**, la raison pour laquelle les appareils ont été ajoutés à la liste des appareils de confiance.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter des appareils de confiance depuis la ligne de commande

1. Pour ajouter des appareils de confiance, exécutez la commande suivante :

   ```
   kesl-control --trusted-devices --add <device ID>
   ```

2. Pour consulter la liste des appareils de confiance du module, exécutez la commande suivante :

   ```
   kesl-control --trusted-devices --list
   ```

Exemple

```
kesl-control --trusted-devices --add WDC_C*
```

Paramètres généraux

Paramètres de détection

Détection d'autres types d'objets

Quelle que soit la configuration des paramètres de Kaspersky Endpoint Security, l'application détecte et bloque toujours les virus, les vers et les chevaux de Troie. Ces programmes peuvent provoquer des dégâts considérables à votre ordinateur.

Vous pouvez également activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les ordinateurs ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky.

Comment configurer la détection des applications que les intrus peuvent utiliser pour endommager les appareils ou les données dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de détection**.
5. Dans le groupe **Détection d'autres types d'objets**, cochez la case **Programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles**.

6. Enregistrez vos modifications.



Paramètres de détection

Comment configurer la détection des applications que les intrus peuvent utiliser pour endommager les appareils ou les données via la ligne de commande

1. Pour configurer la détection des applications que les attaquants peuvent utiliser pour endommager les appareils ou les données, exécutez la commande suivante pour les modules de protection de l'application :

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. Pour vérifier les liens par rapport à la base de données des adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données, exécutez la commande suivante dans le module Protection contre les menaces Internet :

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. Pour vérifier les paramètres actuels de l'application, exécutez la commande suivante :

```
kesl-control --get-app-settings
```

4. Pour vérifier les paramètres actuels de la Protection contre les menaces Internet, exécutez la commande suivante :

```
kesl-control --get-settings 14
```

Paramètres de journalisation des événements

Par défaut, Kaspersky Endpoint Security ne consigne pas les événements relatifs au traitement des objets compactés et non infectés, ni les événements relatifs aux objets non traités par le module Protection contre les fichiers malicieux.

Vous pouvez activer la consignation de ces événements afin que l'application génère les événements *Détection d'un objet compacté*, *Objet non traité* et *Objet traité*. Ces événements peuvent être utiles lors de la configuration du module, ainsi que pour le débogage ou le dépannage de l'application. Cela vous permet de vous assurer que ces objets ont été analysés par l'application et n'ont pas été ignorés en raison d'erreurs.

Comment activer la journalisation des événements de traitement des objets dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de détection**.
5. Sous **Paramètres de journalisation des objets**, cochez les cases en regard des types d'événements concernés.
   - **Journaliser les objets non infectés**
   - **Journaliser les objets non traités**
   - **Journaliser les objets compactés**
6. Enregistrez vos modifications.

Comment activer la journalisation des événements relatifs au traitement des objets en ligne de commande

1. Pour consigner les événements relatifs aux objets non infectés, exécutez la commande suivante :

   ```
   kesl-control --set-settings 1 ReportCleanObjects=Yes
   ```
2. Pour consigner les événements relatifs aux objets non traités, exécutez la commande suivante :

   ```
   kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
   ```
3. Pour consigner les événements relatifs aux objets compactés, exécutez la commande suivante :

   ```
   kesl-control --set-settings 1 ReportPackedObjects=Yes
   ```
4. Pour vérifier les valeurs actuelles des paramètres de la Protection contre les fichiers malicieux, exécutez la commande suivante :

   ```
   kesl-control --get-settings 1
   ```

Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau Kaspersky Security Network permet de récupérer ces données.

La fonctionnalité KSN peut ne pas être disponible dans le logiciel aux États-Unis.

Kaspersky Security Network (KSN) est une infrastructure de service cloud qui permet d'accéder à la base de connaissances de Kaspersky sur la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network permet à Kaspersky Endpoint Security de réagir plus rapidement aux nouvelles menaces, améliore les performances de certains modules de protection et réduit la probabilité de faux positifs. Si vous participez à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés. Pour plus de détails sur la configuration de KSN, consultez l'aide de Kaspersky Security Center.

L'utilisation de Kaspersky Security Network est volontaire. L'application propose d'utiliser le KSN pendant la configuration initiale de l'application. Vous pouvez décider de participer au KSN ou d'interrompre votre participation à tout moment.

Pour en savoir plus sur la soumission des statistiques obtenues pendant la participation à KSN, sur le stockage et la destruction de ces informations, consultez la Déclaration de Kaspersky Security Network et le site de Kaspersky. Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network est inclus dans le paquet de distribution de l'application et est disponible dans le répertoire /opt/kaspersky/kesl/doc.

L'infrastructure des bases de données de réputation de Kaspersky

Kaspersky Endpoint Security prend en charge les solutions d'infrastructure suivantes pour les bases de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques.

- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Endpoint Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KPSN a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :

  - absence de connexion des postes de travail locaux à Internet ;

  - interdiction légale ou restriction de la sécurité de l'entreprise d'envoyer des données en dehors du pays ou du réseau local de l'entreprise.

Après avoir activé une application sous une nouvelle licence, vous devez fournir à votre fournisseur de services les nouvelles informations de clé de licence pour utiliser KPSN. Dans le cas contraire, il sera impossible d'échanger des informations avec KPSN en raison d'une erreur d'authentification.

Limitations de Kaspersky Private Security Network

Kaspersky Private Security Network vous permet d'utiliser votre propre base de données de réputation locale pour vérifier la réputation des objets (fichiers ou adresses Internet). La réputation d'un objet ajouté à la base de données de réputation locale a une priorité plus élevée que celle d'un objet ajouté à KSN/KPSN. Par exemple, imaginez que Kaspersky Endpoint Security analyse un ordinateur et demande la réputation d'un fichier dans KSN/KPSN. Si le fichier a une réputation *Douteuses* dans la base de données de réputation locale, mais a une réputation *De confiance* dans KSN/KPSN, Kaspersky Endpoint Security détectera le fichier comme *Douteuses* et prendra les mesures définies concernant les menaces détectées.

Cependant, dans certains cas, il se peut que Kaspersky Endpoint Security ne demande pas la réputation d'un objet dans KSN/KPSN. Si tel est le cas, Kaspersky Endpoint Security ne recevra pas les données de la base de données de réputation locale de KPSN. Il se peut que Kaspersky Endpoint Security ne demande pas la réputation d'un objet dans KSN/KPSN pour les raisons suivantes :

- Les applications de Kaspersky utilisent des bases de données de réputation hors ligne. Les bases de données de réputation hors ligne sont conçues pour optimiser les ressources pendant le fonctionnement des applications Kaspersky et pour protéger les objets d'importance critique sur l'ordinateur. Les bases de données de réputation hors ligne sont créées par les experts de Kaspersky à partir des données de Kaspersky Security Network. Les applications Kaspersky mettent à jour les bases de données de réputation hors ligne avec les bases antivirus de l'application en question. Si les bases de données de réputation hors ligne contiennent des informations sur un objet en cours d'analyse, l'application ne demande pas la réputation de cet objet à KSN/KPSN.

- Les exclusions d'analyse (zone de confiance) sont configurées dans les paramètres de l'application. Si tel est le cas, l'application ne tient pas compte de la réputation de l'objet dans la base de données de réputation locale.

- L'application utilise des technologies d'optimisation de l'analyse, telles qu'iChecker ou la mise en cache des requêtes de réputation adressées à KSN/KPSN. Si tel est le cas, il se peut que l'application ne demande pas la réputation des objets précédemment analysés.

- Pour optimiser sa charge de travail, l'application analyse les fichiers d'un certain format et d'une certaine taille. La liste des formats et des limites de taille pertinents est déterminée par les experts de Kaspersky. Cette liste est mise à jour avec les bases antivirus de l'application. Vous pouvez également configurer les paramètres d'optimisation de l'analyse dans l'interface de l'application, par exemple pour le module Protection contre les fichiers malicieux .

- Kaspersky Endpoint Security en mode Light Agent communique avec les serveurs KSN via un serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge.

Comment activer ou désactiver Kaspersky Security Network

Par défaut, Kaspersky Endpoint Security utilise le mode étendu du KSN. Le *mode étendu de KSN* est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Endpoint Security envoie des données supplémentaires à Kaspersky.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour en savoir plus sur la soumission des statistiques obtenues pendant la participation à KSN, sur le stockage et la destruction de ces informations, consultez la Déclaration de Kaspersky Security Network et le site de Kaspersky. Le fichier qui reprend la Déclaration de Kaspersky Security Network figure dans le kit de distribution de l'application.

Comment activer ou désactiver KSN dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

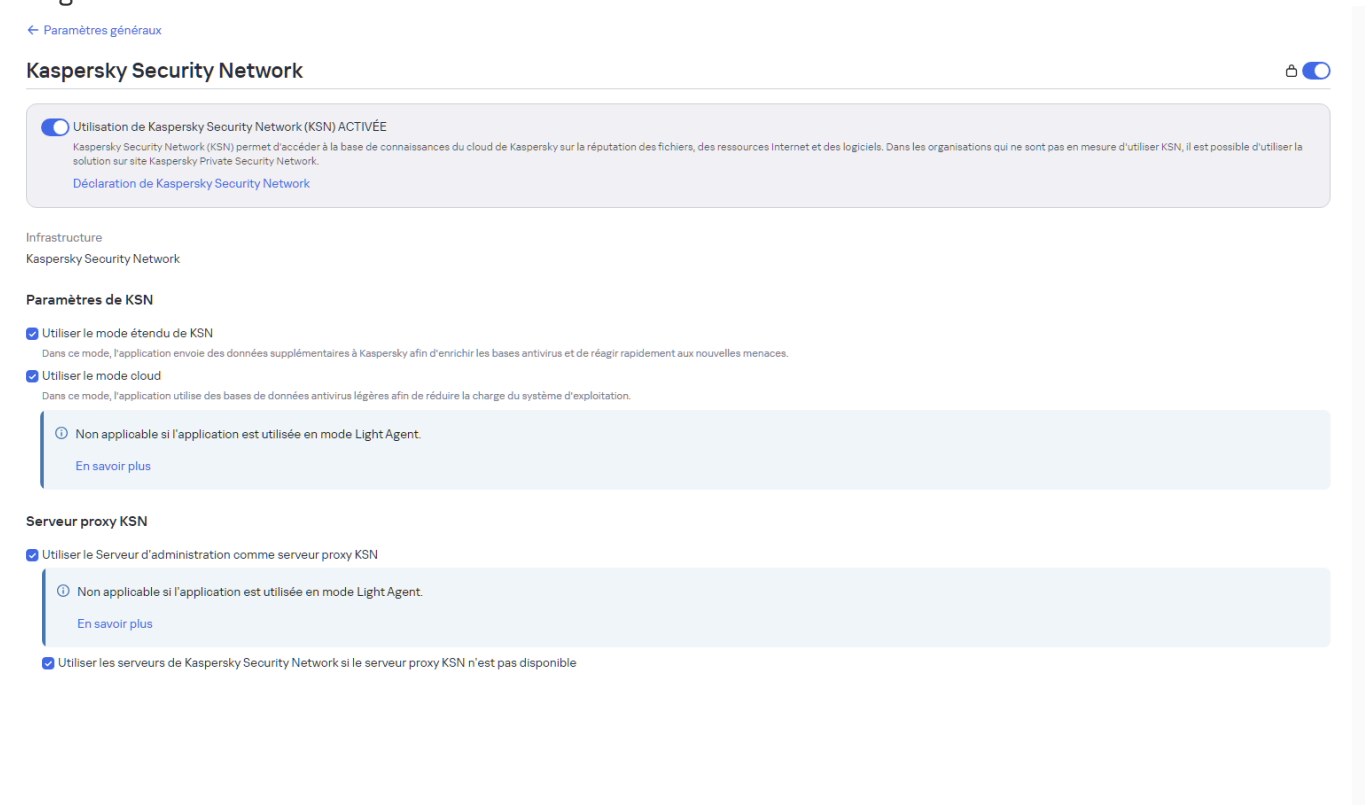
4. Passez à la section **Paramètres généraux** → **Kaspersky Security Network**.

5. Utilisez le bouton bascule **Utilisation de Kaspersky Security Network (KSN)** pour activer ou désactiver le module.

6. Si vous avez activé l'utilisation de KSN, la fenêtre **Déclaration de Kaspersky Security Network** s'ouvre. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.

7. Si nécessaire, cochez ou décochez la case **Utiliser le mode étendu de KSN**.

8. Enregistrez vos modifications.



Kaspersky Security Network

Comment activer ou désactiver KSN en ligne de commande

1. Vérifiez l'état de Kaspersky Security Network :

```
kesl-control --app-info
```

L'application affiche l'état de KSN dans la ligne **Utilisation de Kaspersky Security Network** :

- **Désactivé**
- **Mode KSN de base**
- **Mode étendu de KSN**.

2. Pour activer le mode standard de Kaspersky Security Network, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. Pour activer le mode étendu de KSN, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. Pour désactiver Kaspersky Security Network, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=No
```

Comment activer ou désactiver l'utilisation de KSN dans l'interface de l'application

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre qui s'ouvre, choisissez l'une des options suivantes :
   - **Mode étendu de KSN**, si vous souhaitez utiliser Kaspersky Security Network, obtenir des informations dans la base de connaissances et envoyer des statistiques anonymes ainsi que des informations sur les types et les sources de menaces.
   - **Mode KSN de base**, si vous souhaitez utiliser Kaspersky Security Network, obtenir des informations dans la base de connaissances, mais sans envoyer de statistiques anonymes ni d'informations sur les types et les sources de menaces.
4. Cliquez sur **Activer**.
5. Dans la fenêtre **Utilisation de Kaspersky Security Network**, lisez attentivement la Déclaration de Kaspersky Security Network, puis sélectionnez l'une des options suivantes :
   - **Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network**.
   - **Je n'accepte pas les conditions de la Déclaration de Kaspersky Security Network**.
6. Cliquez sur **OK**.

Par conséquent, si l'utilisation de KSN est activée, Kaspersky Endpoint Security utilise les informations sur la réputation des fichiers, des ressources Internet et des applications reçues de Kaspersky Security Network.

Kaspersky Endpoint Security utilise les paramètres réseau suivants pour communiquer avec les services externes :

Adresse	Protocole	Port
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

Qu'est-ce que le mode Cloud de l'application

En *mode Cloud*, Kaspersky Endpoint Security utilise une version allégée des bases antivirus, ce qui réduit de moitié environ la charge sur la RAM de l'ordinateur.

Le mode Cloud peut être utilisé uniquement lorsque Kaspersky Security Network est activé. Si vous ne participez pas à Kaspersky Security Network ou si le mode cloud est désactivé, Kaspersky Endpoint Security télécharge la version complète des bases de données antivirus depuis les serveurs de Kaspersky. Le mode Cloud est activé par défaut.

Si l'application fonctionne en mode Light Agent, le mode Cloud n'est pas disponible.

Comment activer ou désactiver le mode Cloud dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Kaspersky Security Network**.
5. Utilisez le commutateur **Utiliser le mode cloud** pour activer ou désactiver le module.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le mode Cloud sur la ligne de commande

1. Exécutez la commande permettant d'afficher les paramètres généraux de l'application pour connaître l'état actuel de l'application :

   ```
   kesl-control --get-app-settings
   ```

   L'application affiche son état dans la ligne `CloudMode`.
2. Pour activer ou désactiver le mode Cloud, exécutez la commande suivante :

   ```
   kesl-control --set-app-settings CloudMode=<Yes|No>
   ```

Par conséquent, Kaspersky Endpoint Security télécharge une version allégée ou une version complète des bases antivirus lors de la prochaine mise à jour.

Si la version simplifiée des bases antivirus ne peut être utilisée, Kaspersky Endpoint Security passe automatiquement à l'utilisation de la version complète des bases antivirus.

À quoi sert le proxy KSN

Les ordinateurs des utilisateurs qui sont administrés par le Serveur d'administration de Kaspersky Security Center peuvent interagir avec KSN soit directement, soit via le service KSN Proxy.

Si l'application s'exécute en mode Light Agent, la communication directe avec KSN n'est pas prise en charge. Kaspersky Endpoint Security interagit avec les serveurs KSN à l'aide d'un serveur proxy KSN.

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur peut interroger KSN et transmettre des informations à KSN, même en l'absence d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication avec le réseau externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Par défaut, une fois que KSN est activé et que la Déclaration KSN est acceptée, l'application utilise un serveur proxy pour se connecter à Kaspersky Security Network. Le serveur proxy utilisé par l'application est le Serveur d'administration de Kaspersky Security Center via le port TCP 13111.

Vous pouvez configurer les paramètres du serveur proxy KSN dans les propriétés du Serveur d'administration. Pour en savoir plus sur le serveur proxy KSN, consultez l'aide de Kaspersky Security Center.

La configuration des paramètres de connexion au serveur proxy KSN à l'aide de la ligne de commande n'est pas disponible.

Configuration d'une connexion KSN via un serveur proxy dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux → Kaspersky Security Network**.
5. Utilisez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver l'utilisation du proxy KSN.
6. Le cas échéant, cochez ou décochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**. La case est cochée par défaut.

   Si cette option est activée, Kaspersky Endpoint Security utilise directement les serveurs KSN lorsque le service KSN Proxy n'est pas disponible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).
7. Enregistrez vos modifications.

Configuration de l'envoi des informations vers le stockage de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez activer ou désactiver l'envoi d'informations sur les fichiers de la sauvegarde, les fichiers en quarantaine, les fichiers non traités et les appareils connectés au stockage de Kaspersky Security Center.

Comment consulter les fichiers mis en quarantaine sur les appareils clients

La liste générale des fichiers mis en quarantaine par les applications Kaspersky sur les appareils clients est conservée dans Kaspersky Security Center.

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages**.
2. Accédez au dossier **Quarantaine**.
3. Les informations sur les objets mis en quarantaine s'affichent dans le volet droit de la console.

Comment consulter les fichiers de la Sauvegarde sur les appareils clients

La liste générale des fichiers placés dans la Sauvegarde par les applications Kaspersky sur les appareils clients est conservée dans Kaspersky Security Center.

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages**.
2. Accédez au dossier **Sauvegardes de fichiers**.
3. Les informations sur les objets placés dans la Sauvegarde s'affichent dans le volet droit de la console.

Comment consulter les informations sur les fichiers non traités dans la liste des menaces actives

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages**.
2. Accédez au dossier **Menaces actives**.
3. Les informations sur les fichiers non traités dans la liste des menaces actives s'affichent dans le volet droit de la console.

Comment consulter les informations sur le matériel connecté aux appareils clients

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages**.
2. Accédez au dossier **Matériel**.
3. Les informations sur les appareils s'affichent dans le volet droit de la console.

Les informations sont transmises si le module Contrôle des appareils est activé.

Comment consulter les informations sur les applications sur les appareils clients

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Applications tierces**.
2. Accédez au dossier **Registre des applications**.
3. Les informations sur les applications s'affichent dans le volet droit de la console.

Les informations sont transmises si le module Contrôle des applications est activé.

Comment configurer l'intégration au Serveur d'administration

Pour configurer l'intégration au Serveur d'administration dans les propriétés de la stratégie :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux → Intégration KSC**.
5. Cliquez sur le lien **Paramètres complémentaires**.
6. Sélectionnez les catégories d'événements sur les ordinateurs clients dont les informations doivent être transmises au Serveur d'administration :
   - **À propos des fichiers en quarantaine** Cette case à cocher active ou désactive le transfert des informations relatives aux fichiers mis en quarantaine vers le Serveur d'administration.
   - **À propos des fichiers de la Sauvegarde**. La case à cocher active ou désactive le transfert des informations sur les fichiers de la sauvegarde vers le Serveur d'administration.
   - **À propos des fichiers non traités**. La case active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration.
   - **À propos des appareils installés**. La case active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci.
   - **À propos des applications lancées**. La case active ou désactive la transmission au Serveur d'administration de la liste des applications détectées sur l'appareil client à la suite de la tâche d'inventaire.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Pour configurer l'intégration au Serveur d'administration dans les propriétés d'un appareil administré :

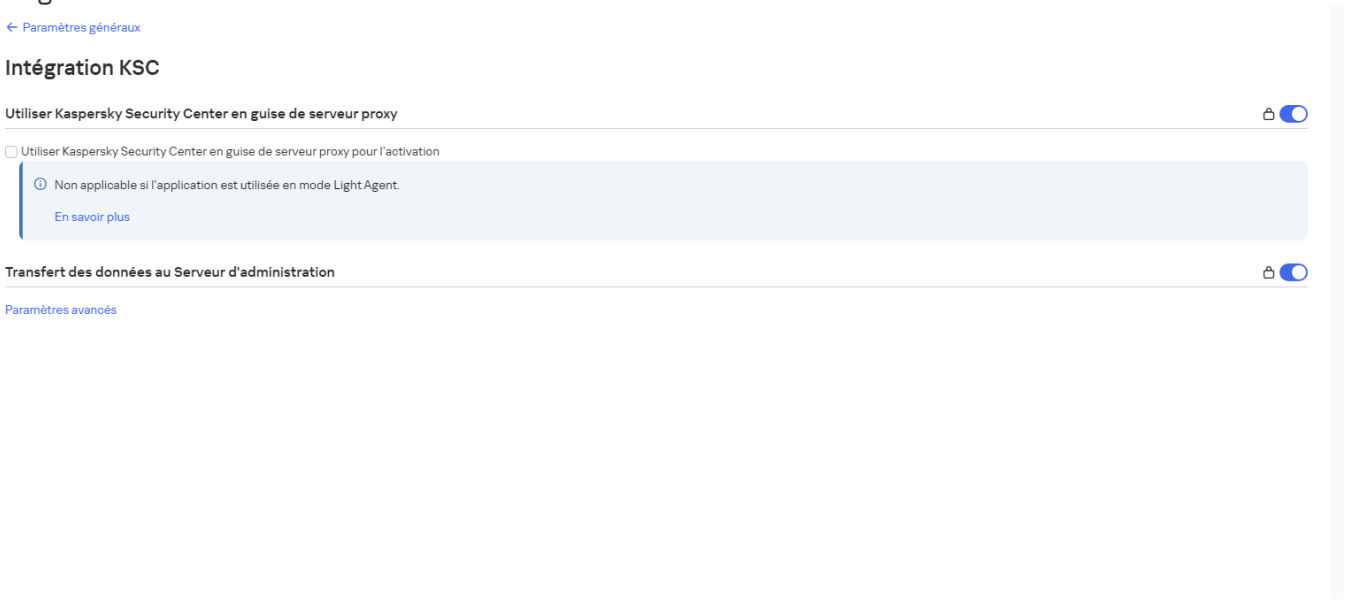
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (appareils) → Appareils administrés**.
2. Cliquez sur le lien **<device name>**.
3. Sélectionnez l'onglet **Applications** et cliquez sur le lien **Kaspersky Endpoint Security**.
4. Sous l'onglet **Paramètres de l'application**, accédez à la section **Paramètres de stockage**.

5. Sous **Paramètres de transfert de données vers le Serveur d'administration**, cliquez sur le bouton **Configurer**.

6. Dans la fenêtre **Paramètres de transfert de données**, vous pouvez activer ou désactiver l'envoi d'informations au Serveur d'administration :

   - **Signaler les fichiers dans la Sauvegarde**. La case à cocher active ou désactive le transfert des informations sur les fichiers de la sauvegarde vers le Serveur d'administration.
   - **Signaler les fichiers en quarantaine**. La case à cocher active ou désactive le transfert des informations sur les fichiers mis en quarantaine vers le Serveur d'administration.
   - **Signaler les fichiers non traités**. La case active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration.
   - **Signaler les appareils installés**. La case active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci.
   - **Signaler les applications trouvées sur l'appareil**. La case active ou désactive la transmission au Serveur d'administration de la liste des applications détectées sur l'appareil client à la suite de la tâche d'inventaire.

7. Enregistrez vos modifications.



Intégration à Kaspersky Security Center

Comment configurer le lancement de l'application

Configuration du lancement de l'application

Vous pouvez configurer le nombre maximal de tentatives de lancement infructueuses et le délai d'expiration du lancement de Kaspersky Endpoint Security. Cela permet de réduire la charge sur le système si l'application ne peut pas démarrer pendant une longue période. Par défaut, le nombre maximal de tentatives consécutives infructueuses de lancement de l'application est de 5 et le délai d'expiration maximal est de 3 minutes.

Comment configurer le lancement de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux → Interaction avec l'utilisateur**.
5. Sous **Paramètres de démarrage de l'application**, saisissez des valeurs dans les champs suivants :
   - **Nombre maximum de tentatives consécutives infructueuses pour démarrer une application**. Valeur par défaut : 5.
   - **Durée maximale d'attente pour le démarrage de l'application (min)**. Valeur par défaut : 3.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer le lancement de l'application via la ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de démarrage de l'application à l'aide des paramètres `MaxRestartCount` et `StartupTimeout` dans le fichier de configuration kesl.ini.

Le paramètre `MaxRestartCount` permet de définir le nombre maximum de tentatives consécutives infructueuses de démarrage d'une application. Le paramètre peut prendre des valeurs de 1 à 10. Valeur par défaut : 5.

Le paramètre `StartupTimeout` permet de définir le temps maximum d'attente avant le démarrage de l'application (en minutes), après quoi le processus kesl sera redémarré. Le paramètre peut prendre des valeurs de 1 à 60. Valeur par défaut : 3.

Application des mises à jour critiques

Vous pouvez configurer l'application pour qu'elle redémarre automatiquement à la réception de mises à jour critiques. Par défaut, l'application redémarre automatiquement si des mises à jour critiques sont reçues lors de la première mise à jour des bases de données et des modules dans les 24 heures suivant son installation.

Configuration du redémarrage automatique de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux → Interaction avec l'utilisateur**.

5. Dans le groupe **Installation des mises à jour critiques**, cochez la case **Redémarrer automatiquement l'application lorsque des mises à jour critiques sont reçues**.

   Kaspersky Endpoint Security redémarre automatiquement à la réception de mises à jour critiques.

6. Enregistrez vos modifications.

Comment configurer le redémarrage automatique de l'application via la ligne de commande

Vous pouvez configurer le redémarrage automatique de l'application via la ligne de commande à l'aide du paramètre `UrgentUpdateRestartEnabled` dans les paramètres généraux de l'application.

Pour redémarrer automatiquement l'application lors de l'installation de mises à jour critiques, exécutez la commande suivante :

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

Configuration des autorisations de gestion des tâches

Dans Kaspersky Security Center, vous pouvez configurer les autorisations suivantes pour les utilisateurs :

- autorisation d'utiliser les tâches locales créées dans l'application Kaspersky Endpoint Security. Si la stratégie de Kaspersky Security Center empêche les utilisateurs de consulter, de modifier ou de supprimer les tâches locales, les informations relatives aux tâches Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (en mode standard) et Rollback (en mode standard) ne sont pas disponibles.

- autorisation d'afficher et de gérer les tâches créées dans Kaspersky Security Center sur les appareils clients.

Pour configurer les autorisations de gestion des tâches dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.

5. Sous **Actions autorisées**, sélectionnez les actions que les utilisateurs sont autorisés à exécuter sur leurs appareils :

   - **Accéder aux tâches locales**. Si la case est cochée, les tâches locales sont affichées dans l'interface locale de Kaspersky Endpoint Security. Si aucune autre restriction de la stratégie ne s'y oppose, les utilisateurs peuvent configurer, exécuter, créer et supprimer les tâches locales disponibles dans l'interface graphique de l'application ou sur la ligne de commande.

   - **Gérer les tâches de groupe**. Si cette case est cochée, les utilisateurs peuvent administrer les tâches de groupe configurées dans Kaspersky Security Center sur les appareils clients. Les tâches peuvent être lancées depuis l'interface graphique de l'application ou sur la ligne de commande.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Protection par mot de passe

La Protection par mot de passe permet de restreindre l'accès des utilisateurs à la modification de Kaspersky Endpoint Security conformément aux autorisations accordées (par exemple, l'autorisation de consulter les rapports de l'application). La restriction de l'accès aux paramètres de l'application réduit le risque de modifications non autorisées ou involontaires de l'application.

Fonctionnement de la Protection par mot de passe

1. **Un utilisateur tente d'exécuter une action contrôlée par le module**

   Par exemple, désactiver des modules de protection ou consulter les rapports de Kaspersky Endpoint Security.

2. **Kaspersky Endpoint Security vérifie les droits de l'utilisateur**

   Si l'utilisateur dispose de l'autorisation correspondante, l'action est exécutée avec succès. Si l'utilisateur ne dispose pas de l'autorisation correspondante, l'application bloque l'action et affiche une erreur.

   Dans l'interface graphique de Kaspersky Endpoint Security, les actions interdites ne peuvent pas être affichées ni modifiées.

Configuration de la Protection par mot de passe

1. **Activer la Protection par mot de passe**

   Par défaut, la Protection par mot de passe est désactivée. Activez le module dans Web Console ou dans la Console d'administration, ou via la ligne de commande à l'aide de la commande suivante :

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **Configurer les autorisations des utilisateurs**

   Par défaut, les autorisations des utilisateurs sont configurées dans l'application pour les groupes d'utilisateurs prédéfinis : *kesladmin*, *kesluser*, *keslaudit*.

   Configurez les autorisations des utilisateurs pour ces groupes ou créez un utilisateur ou un groupe d'utilisateurs.

   > Pour que l'application fonctionne correctement, nous vous recommandons de configurer les autorisations pour au moins un groupe.

   Comment configurer des autorisations personnalisées dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux → Autodéfense**.

5. Assurez-vous que le commutateur du module est en position **Protection par mot de passe ACTIVÉE**.

6. Cliquez sur le lien **Autorisations utilisateur**.

   Cette action ouvre une fenêtre contenant les utilisateurs et leurs autorisations.

7. Si vous souhaitez modifier les autorisations des groupes prédéfinis, cliquez sur le nom d'un groupe.

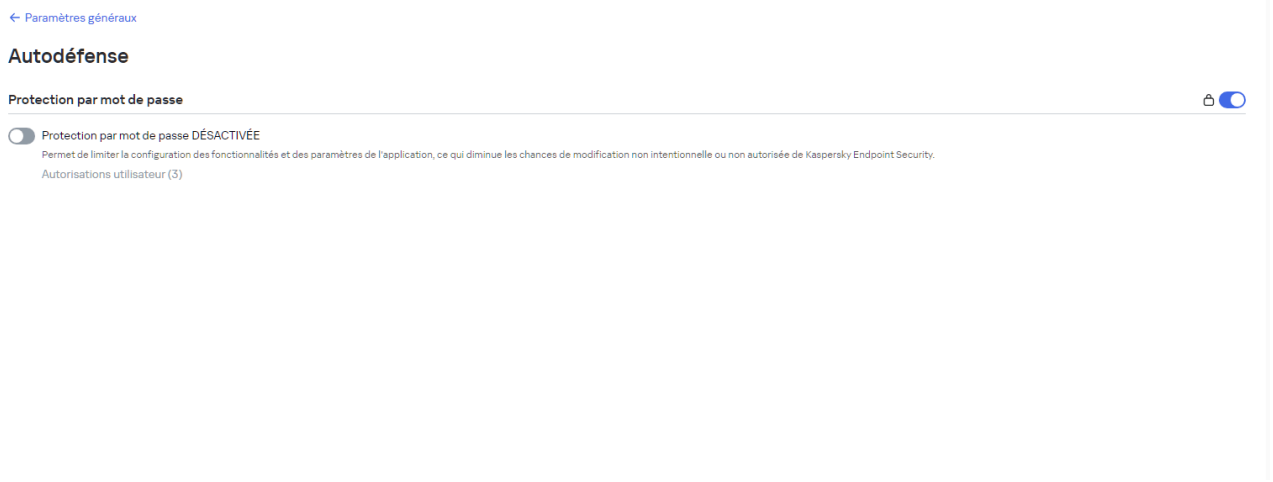
   Si vous souhaitez modifier les autorisations d'un autre utilisateur ou groupe :

   a. Cliquez sur **Ajouter**.

   b. Sélectionnez un utilisateur ou un groupe dans Active Directory ou saisissez le nom manuellement.

8. Cochez les cases en regard des autorisations que vous souhaitez accorder à l'utilisateur ou au groupe.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Autodéfense

Comment configurer des autorisations personnalisées via la ligne de commande

1. Pour afficher la liste des paramètres actuels de la Protection par mot de passe, exécutez la commande suivante :

```
kesl-control --get-permission-manager-settings
```

2. Pour modifier les autorisations d'un utilisateur ou d'un groupe, exécutez la commande suivante :

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. Pour supprimer un utilisateur ou un groupe pour lequel des autorisations ont été configurées, exécutez la commande suivante :

```
kesl-control --remove-permissions <principal> [--group]
```

Symboles

Options de la commande

Paramètre	Description
`--group`	Le paramètre s'applique à un groupe. Si l'option `--group` n'est pas spécifiée, le paramètre s'applique à un utilisateur individuel.
`--file <file name>`	Exportation des paramètres dans un fichier ou importation des paramètres depuis un fichier. Saisissez une valeur `<file name>`.
`--json`	Exportation des paramètres dans un fichier JSON ou importation des paramètres depuis un fichier JSON. Cette option ne peut être spécifiée que si l'option `--file <file name>` est spécifiée.
`principal`	Nom de l'utilisateur ou du groupe d'utilisateurs.
`permissions`	Autorisations personnalisées. Spécifiez `Yes` pour autoriser une action à l'utilisateur, ou `No` pour la refuser. • `StopProtection`. Désactivation des modules de protection. • `StopSecurityControl`. Désactivation des modules de contrôle • `StartProtection`. Activation des modules de protection. • `StartSecurityControl`. Activation des modules de contrôle • `ApplicationSettings`. Configuration de l'application • `ViewReports`. Consulter les rapports • `RestoreFromBackup`. Restauration depuis la Sauvegarde • `RemoveLicenseKey`. Suppression de la clé • `AddLicense`. Ajout d'une clé • `DisablePolicy`. Désactivation de la stratégie de Kaspersky Security Center

Exemples

Révoquer l'autorisation de consulter les rapports au groupe *kesluser* :

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

Autoriser *new-user* à gérer les modules de contrôle :

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

Considérations particulières relatives à la Protection par mot de passe

- Si la Protection par mot de passe est désactivée, l'autorisation de l'utilisateur à administrer l'application est déterminée par les rôles des utilisateurs.
- Si le niveau d'accès d'un utilisateur est régi à la fois par des autorisations de groupe et par des autorisations individuelles, les autorisations individuelles prévalent sur les autorisations de groupe. Autrement dit, même si les autorisations individuelles d'un utilisateur sont plus restrictives que les autorisations de groupe du même utilisateur, les autorisations les plus restrictives prévalent.

  Par exemple, si l'administration de l'application est interdite au groupe *kesluser*, vous pouvez tout de même autoriser l'administration de l'application à un utilisateur individuel membre de ce groupe. Cet utilisateur est toujours autorisé à administrer l'application, même si les autorisations de groupe ne le permettent pas.
- Si la Protection par mot de passe est activée et qu'un utilisateur ne dispose ni d'autorisations individuelles ni d'autorisations de groupe, toutes les actions sont interdites.

À propos des autorisations personnalisées

Si la Protection par mot de passe est activée, l'accès à l'administration de Kaspersky Endpoint Security est contrôlé à l'aide des *autorisations utilisateur*. Les autorisations utilisateur définissent les droits d'un utilisateur (voir le tableau ci-dessous).

Autorisations personnalisées

Autorisation	Autorisations
Configuration de l'application	Consultation et modification des paramètres de l'application. Gestion des paramètres des tâches dans l'interface graphique de l'application et en ligne de commande sans utiliser la commande `sudo`. Attribuer n'importe quel rôle à n'importe quel utilisateur. Attribuer et révoquer un rôle à n'importe quel utilisateur (l'administrateur ne peut pas révoquer le rôle d'admin de lui-même). Gestion de la tâche *Annulation de la mise à jour des bases*. Gestion des modules : • Managed Detection and Response • Endpoint Detection and Response Optimum
Activation des modules de protection.	Gestion des modules : • Protection contre les fichiers malicieux • Analyse des disques amovibles • Détection comportementale • Protection contre le chiffrement • Protection BadUSB • Protection contre les menaces par emails • Protection contre les menaces Internet • Protection contre les menaces réseau • Gestion du pare-feu • Contrôle de l'intégrité du système • Prévention de l'exécution des objets (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Intégration avec KUMA
Désactivation des modules de protection	
Activation des modules de contrôle	Gestion des modules : • Contrôle des appareils • Contrôle des applications • Contrôle Internet
Désactivation des modules de contrôle	
Consulter les rapports	Consultation des rapports des tâches Consultation des événements
Restauration depuis la Sauvegarde	Afficher et gérer les stockages des utilisateurs.
Suppression de la clé	Gérer les licences d'application.
Ajout d'une clé	
Désactivation de la stratégie de Kaspersky Security Center	Désactivation ou activation de la stratégie de Kaspersky Security Center sur l'appareil.

Particularités liées aux autorisations personnalisées

- Les autorisations utilisateur n'affectent pas la consultation de la liste des tâches, la consultation des objets dans la Sauvegarde, ni la consultation des paramètres et de l'état de l'application.

Tous les utilisateurs sont autorisés à gérer les tâches suivantes :

- Tâches d'analyse (*Analyse personnalisée*, *Analyse du conteneur*, *Analyse personnalisée du conteneur*, *Analyse des zones critiques*, *Analyse des logiciels malveillants*)
- *Inventaire*
- *Mise à jour des bases et modules d'application*
- *vérification de l'intégrité du système.*
- *Recherche d'IoC*

- Vous ne pouvez pas ajouter ni supprimer la clé de licence principale dans l'interface graphique si l'appareil est contrôlé par une stratégie de Kaspersky Security Center. Un utilisateur disposant des autorisations *Ajout d'une clé* et *Supprimer la clé* peut ajouter une clé de réserve ou une clé de licence pour activer d'autres solutions de Kaspersky (module complémentaire).

  Si l'appareil n'est pas administré par une stratégie, l'utilisateur peut supprimer ou ajouter la clé de licence principale.

Autorisations utilisateur par défaut

Par défaut, les autorisations des utilisateurs sont configurées dans l'application pour les groupes d'utilisateurs prédéfinis : *kesladmin*, *kesluser*, *keslaudit*. Pour les utilisateurs qui ne sont pas membres de ces groupes, toutes les opérations avec l'application sont interdites.

Autorisations utilisateur des groupes prédéfinis

Autorisation	kesladmin	kesluser	keslaudit
Configuration de l'application	✓	–	–
Activation des modules de protection.	✓	–	–
Désactivation des modules de protection	✓	–	–
Activation des modules de contrôle	✓	–	–
Désactivation des modules de contrôle	✓	–	–
Consulter les rapports	✓	–	✓
Restauration depuis la Sauvegarde	✓	–	–
Suppression de la clé	✓	–	–
Ajout d'une clé	✓	–	–
Désactivation de la stratégie de Kaspersky Security Center	✓	–	–

Paramètres de performance

L'analyse de l'ordinateur à l'aide de l'application Kaspersky Endpoint Security peut mobiliser d'importantes ressources système. Pour optimiser la charge du système, vous pouvez :

- Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie
- Limiter la consommation de ressources du processeur pour les tâches d'analyse (%)

- Limiter l'utilisation de la mémoire résidente par l'application
- Exclure la mémoire de certains processus de l'analyse

Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie

Si votre appareil fonctionne sur batterie et que vous souhaitez réduire l'utilisation des ressources par Kaspersky Endpoint Security, vous pouvez ignorer les tâches planifiées :

- Toutes les tâches d'analyse (analyse personnalisée, Analyse du conteneur, Analyse personnalisée du conteneur, analyse des zones critiques, *Analyse des logiciels malveillants*)
- *Inventory*
- *Mise à jour des bases et modules d'application*
- *Vérification de l'intégrité de l'application*
- *Analyse IOC*

Vous pouvez exécuter les tâches requises manuellement.

Comment annuler les tâches planifiées lors du fonctionnement sur batterie à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Performances**.
5. Activez la fonctionnalité **Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie**.
   Kaspersky Endpoint Security *annule* les tâches planifiées.
6. Enregistrez vos modifications.

Comment annuler les tâches planifiées lors du fonctionnement sur batterie à l'aide de la ligne de commande

Dans la ligne de commande, vous pouvez configurer l'annulation des tâches planifiées dans les à l'aide du paramètre `PowerSaveMode` dans les paramètres généraux de l'application.

Pour annuler les tâches planifiées lorsque l'appareil fonctionne sur batterie, exécutez la commande suivante :

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

Limiter la consommation de ressources du processeur pour les tâches d'analyse (%)

Vous pouvez limiter l'utilisation du processeur et de la mémoire pour les tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse du conteneur* (des types ODS, ContainerScan et InventoryScan). Par défaut, la limite d'utilisation de la mémoire est définie sur 8192 Mo. Aucune limite n'est définie pour l'utilisation du processeur.

Il est recommandé de définir la limite d'utilisation de la mémoire pour les tâches d'analyse en dessous de la limite d'utilisation de la mémoire résidente afin que les tâches d'analyse ne consomment pas toute la mémoire vive disponible et ne provoquent pas le redémarrage de l'application.

Notez que la capacité combinée de tous les cœurs de processeur est considérée comme égale à 100 %.

L'utilitaire `top` affiche la charge du processeur, en supposant que la ressource d'un cœur est de 100 %. Ainsi, une valeur de 400 % pour un processeur à 10 cœurs (soit un total de 1 000 % mesuré par l'utilitaire `top`) signifie que l'ensemble du processeur (tous les cœurs au total) est utilisé à 40 %. Si vous voulez que la valeur dans la sortie de l'utilitaire `top` ne dépasse jamais 150 % sur les mêmes 10 cœurs, définissez une limite d'utilisation du processeur de `15%`.

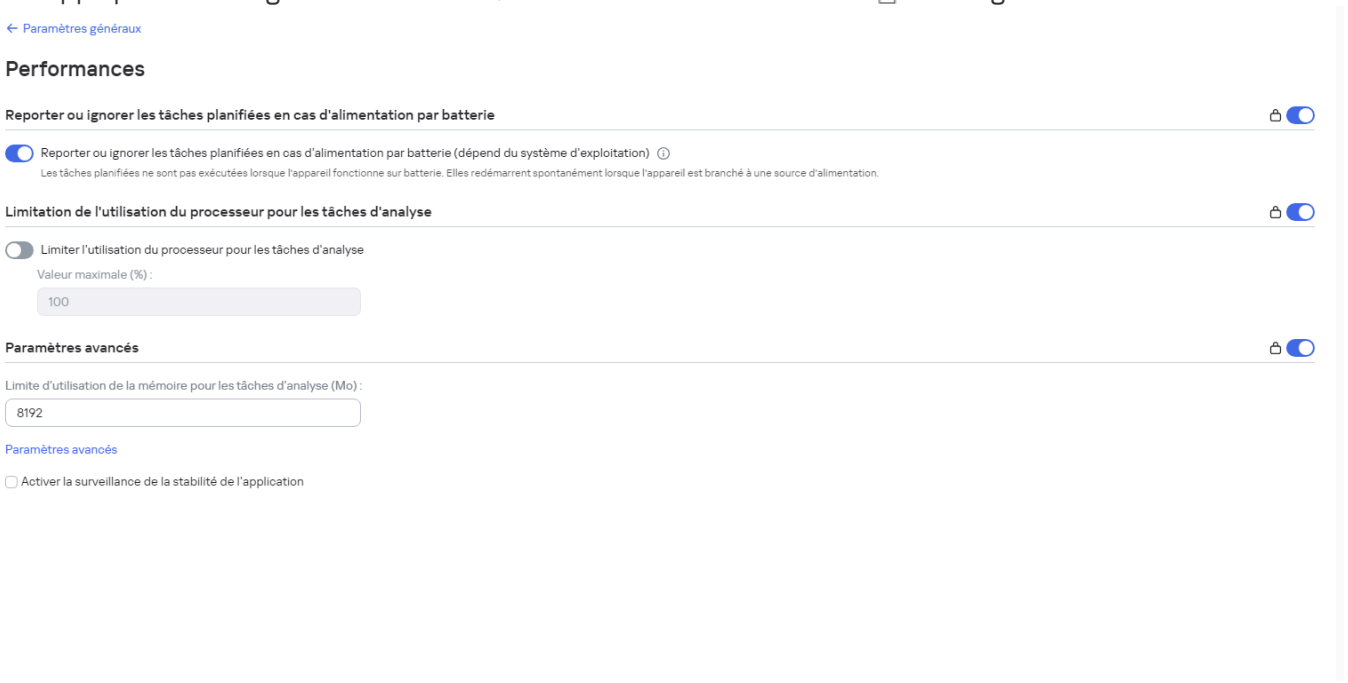
La limite d'utilisation du processeur s'applique aux tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse du conteneur*, ce qui signifie que l'utilisation du processeur peut dépasser la valeur configurée.

La limitation de l'utilisation du processeur n'est pas possible sur les appareils exécutant CentOS 5.2 et 5.4.

Comment limiter l'utilisation des ressources de la mémoire et du processeur dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Performances**.
5. Activez la fonctionnalité **Limitation de l'utilisation du processeur pour les tâches d'analyse**.
6. Spécifiez la charge maximale de tous les cœurs de processeur dans le champ **Valeur maximale (%)**. La valeur doit être un entier compris entre 10 et 100.
7. Dans la section **Paramètres avancés**, spécifiez la limite d'utilisation de la mémoire pour les tâches d'analyse (Mo) dans le champ correspondant. Valeur par défaut : 8192.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Performances

Comment limiter l'utilisation de la mémoire et des ressources du processeur sur la ligne de commande

Sur la ligne de commande, vous pouvez configurer une limite d'utilisation des ressources du processeur pour les tâches d'analyse à l'aide des paramètres `UseOnDemandCPULimit` et `OnDemandCPULimit` dans les paramètres généraux de l'application.

1. Activez la limite d'utilisation du processeur pour les tâches d'analyse en exécutant la commande suivante :

   ```
   kesl-control --set-app-settings UseOnDemandCPULimit = Yes
   ```

2. Définissez une limite d'utilisation du processeur en exécutant la commande suivante :

   ```
   kesl-control --set-app-settings OnDemandCPULimit =<value>
   ```

   La limite est définie sous forme de pourcentage ; les valeurs possibles sont des entiers compris entre 10 et 100.

3. Spécifiez la limite d'utilisation de la mémoire pour les tâches d'analyse en gérant le paramètre `ScanMemoryLimit` dans le fichier de configuration kesl.ini.

Limiter l'utilisation de la mémoire résidente par l'application

Vous pouvez limiter l'utilisation de la mémoire résidente par l'application. Par défaut, la limite est définie à 50 % maximum de la mémoire, mais pas moins de 2 Go et pas plus de 16 Go.

Comment limiter l'utilisation de la mémoire résidente dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux → Performances**.

5. Dans la section **Paramètres avancés**, cliquez sur le lien **Paramètres avancés** et, dans la fenêtre qui s'affiche, cochez la case **Limiter l'utilisation de la mémoire par l'application**.

   Dans la liste déroulante, vous pouvez sélectionner comment limiter l'utilisation de la mémoire résidente :

   - **Définir une valeur exacte (%)**. Lorsque cet élément est sélectionné, le champ **Valeur exacte (%)** devient disponible, dans lequel vous pouvez spécifier une valeur en pourcentage. Valeur par défaut : 50%.
   - **Définir une valeur exacte (Mo)**. Lorsque cet élément est sélectionné, le champ **Valeur exacte (Mo)** devient disponible, dans lequel vous pouvez spécifier une valeur en mégaoctets. La valeur par défaut est 2000 Mo.
   - **Utiliser la plus élevée des deux valeurs (% ou Mo)**. Lorsque cet élément est sélectionné, les champs **Valeur exacte (%)** et **Valeur exacte (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs nécessaires.
   - **Utiliser la plus petite des deux valeurs (% ou Mo)**. Lorsque cet élément est sélectionné, les champs **Valeur exacte (%)** et **Valeur exacte (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs nécessaires.
   - **Limitée automatiquement (recommandé)**. Lorsque vous sélectionnez cet élément de la liste, l'utilisation de la mémoire résidente est automatiquement limitée (par défaut).

6. Enregistrez vos modifications.

Pour appliquer les modifications, redémarrez l'application Kaspersky Endpoint Security sur l'appareil administré après l'application de la stratégie.

Comment limiter l'utilisation de la mémoire résidente sur la ligne de commande

Vous ne pouvez pas gérer le paramètre `MaxMemory` sur la ligne de commande. Utilisez le fichier de configuration kesl.ini pour configurer la limite de la mémoire résidente.

Il est conseillé de modifier les valeurs par défaut en suivant les instructions du Support technique.

Le paramètre `MaxMemory` peut prendre les valeurs suivantes :

- `off` : l'utilisation de la mémoire résidente n'est pas limitée.
- `<value>%` – valeur comprise entre 1 et 100 % de la mémoire RAM.
- `<value>MB` – valeur en mégaoctets.
- `lowest/<value>%/<value>MB` – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets.
- `highest/<value>%/<value>MB` – la plus grande des deux : la valeur en pourcentage et la valeur absolue en mégaoctets.
- `auto` (par défaut) – limite automatique.

Exclure la mémoire de processus de l'analyse

Vous pouvez exclure de l'analyse la mémoire des processus sélectionnés.

Comment exclure la mémoire des processus de l'analyse dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Performances**.
5. Dans le groupe **Paramètres avancés**, cliquez sur le lien **Configurer l'exclusion de l'analyse de la mémoire du processus**.
6. Une fenêtre s'ouvre ; dans cette fenêtre, cliquez sur le bouton **Ajouter** et spécifiez le chemin d'accès au fichier exécutable du processus.
   Exigences relatives au chemin d'accès :
7. Doit commencer par `/` (chemin absolu)
   a. Ne doit pas contenir de caractères interdits :
   - `\0` (octet nul) : interdit par le système d'exploitation.
   - Barre oblique (`/`) dans un nom de fichier ou de répertoire : utilisée comme séparateur.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exclure la mémoire des processus de l'analyse dans la ligne de commande

Dans la ligne de commande, vous pouvez configurer l'exclusion de la mémoire de processus de l'analyse à l'aide du paramètre `MemScanExcludedProgramPath.item_#` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `MemScanExcludedProgramPath.item_#` contient le chemin complet du processus dans le répertoire local. Vous pouvez utiliser des masques pour spécifier le chemin.

Vous pouvez spécifier plusieurs processus dont vous souhaitez exclure la mémoire de l'analyse.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Optimisation de l'utilisation des ressources par l'application

Paramètres du réseau

Vous pouvez configurer le serveur proxy utilisé pour la connexion Internet, sélectionner le mode de surveillance des ports réseau et mettre en place l'analyse des connexions chiffrées.

Comment gérer les paramètres du proxy

Vous pouvez configurer les paramètres du serveur proxy si les utilisateurs des appareils clients accèdent à Internet via un serveur proxy. L'application Kaspersky Endpoint Security peut utiliser un serveur proxy pour se connecter aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites à l'aide du module Protection contre les menaces Internet.

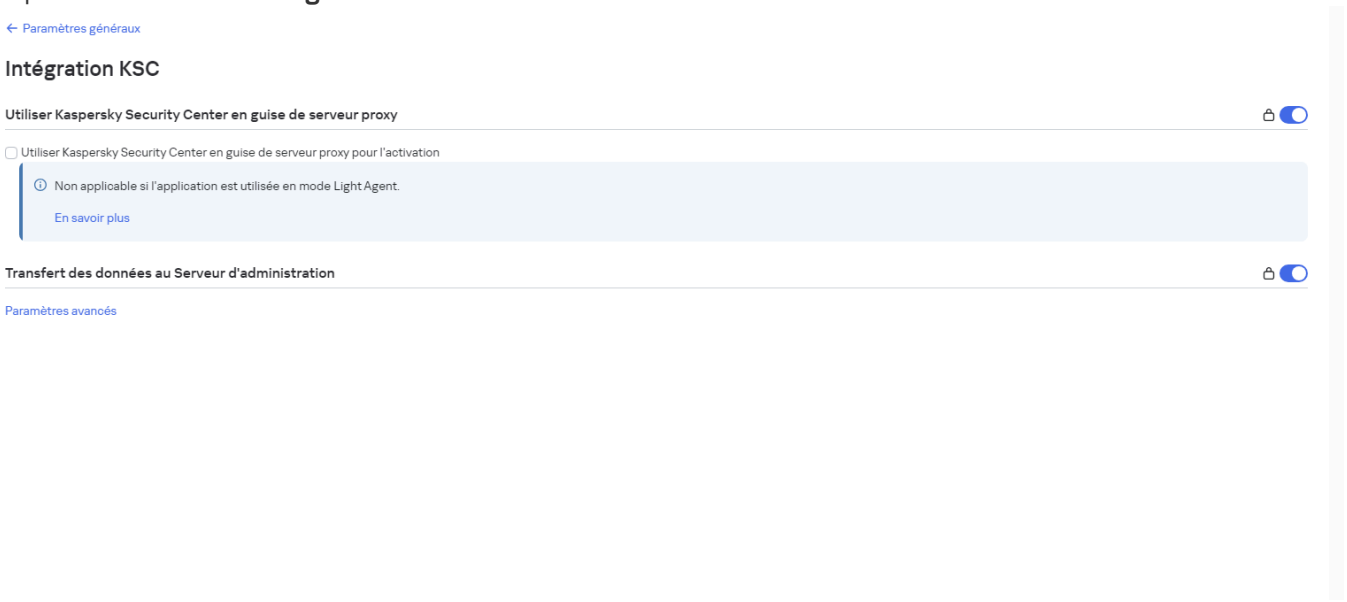
Par défaut, l'utilisation d'un serveur proxy est désactivée.

Si vous activez des appareils situés dans un segment isolé du réseau sans accès à Internet à l'aide d'un code d'activation, vous pouvez utiliser le Serveur d'administration de Kaspersky Security Center comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky.

Comment configurer l'utilisation de Kaspersky Security Center comme serveur proxy pour l'activation de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Accédez à la section **Paramètres généraux → Intégration KSC**.
5. Cochez la case **Utiliser Kaspersky Security Center comme serveur proxy pour l'activation**.

6. Cliquez sur le bouton **Enregistrer**.



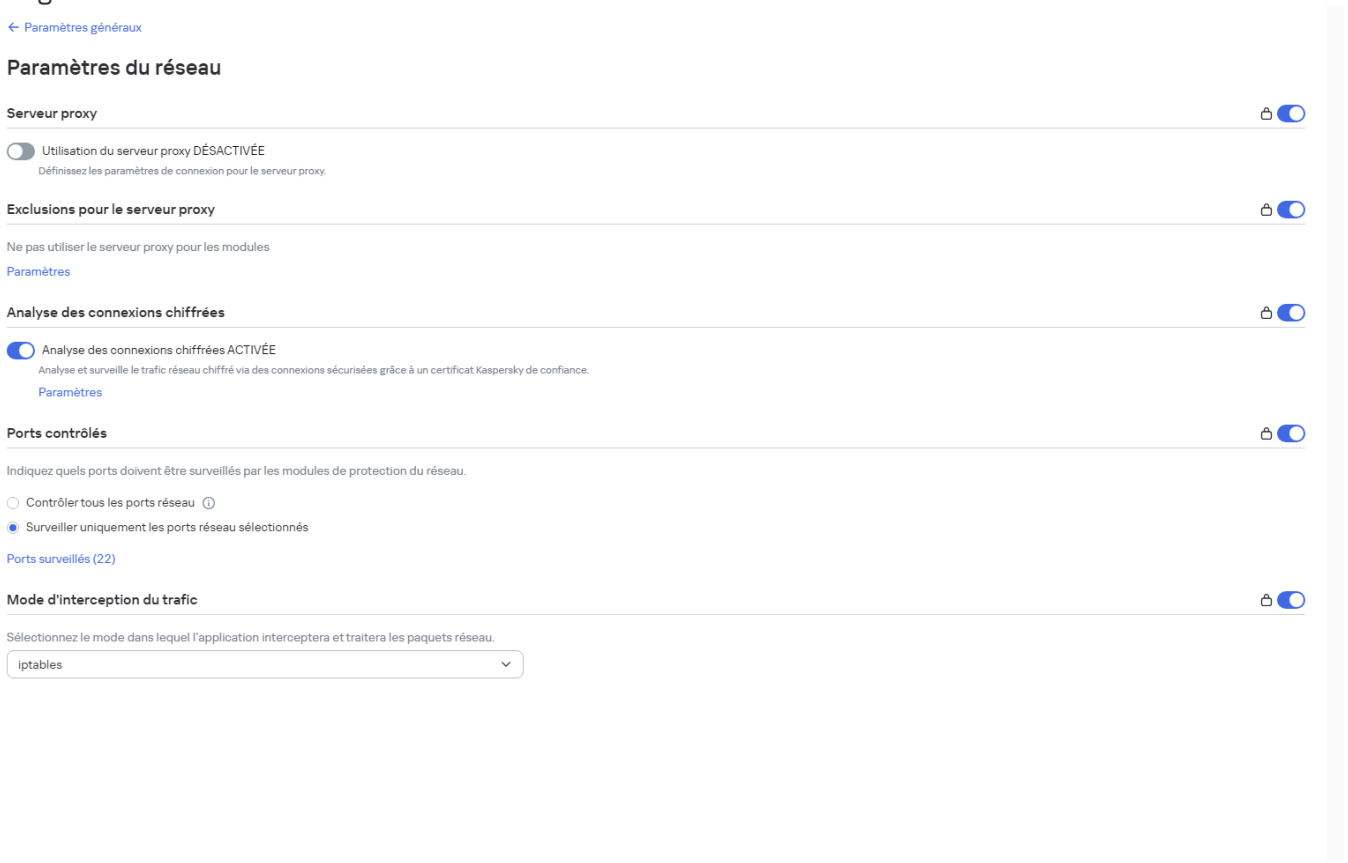
Intégration à Kaspersky Security Center

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'utilisation d'un serveur proxy pour la connexion à Kaspersky Security Network, à la SVM et au Serveur d'intégration n'est pas prise en charge. De plus, l'utilisation du Serveur d'administration comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky n'est pas prise en charge en mode Light Agent.

Comment gérer les paramètres du proxy dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Réglez le commutateur sur **Utilisation du serveur proxy ACTIVÉE**.
6. Dans la fenêtre qui s'affiche, remplissez les champs :
   - **Adresse du serveur proxy**.
   - **Port du serveur proxy**.
7. Si nécessaire, activez l'authentification du serveur proxy :
   a. Cochez la case **Utiliser l'authentification sur le serveur proxy**.
   b. Remplissez les champs :
      - **Nom d'utilisateur**.
      - **Mot de passe**.

8. Enregistrez vos modifications.



Paramètres du réseau

Comment gérer les paramètres du proxy dans la ligne de commande

1. Pour activer l'utilisation d'un serveur proxy, exécutez la commande suivante :

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. Pour vérifier les valeurs actuelles des paramètres réseau, exécutez la commande suivante :

```
kesl-control --get-net-settings
```

Symboles

Options de la commande

Paramètre	Description
`ProxyServer`	Adresse du serveur proxy à utiliser pour la connexion à Internet. Adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.

Exclusions pour le serveur proxy

Si vous n'avez pas besoin d'utiliser un serveur proxy pour les connexions à certaines adresses, vous pouvez ajouter ces adresses aux exclusions.

Vous pouvez également désactiver l'utilisation d'un serveur proxy pour les modules EDR Expert (on-premises), NDR (KATA) et Sandbox, qui assurent l'intégration avec les solutions Detection and Response. Lors de la connexion aux serveurs d'intégration de ces modules, le serveur proxy n'est pas utilisé.

Configuration des exclusions du serveur proxy dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Dans le groupe **Exclusions pour le serveur proxy**, cliquez sur le lien **Paramètres**.

   La fenêtre des exclusions du serveur proxy s'ouvre
6. Cochez les cases des modules avec lesquels vous ne souhaitez pas utiliser de serveur proxy :
   - **Endpoint Detection and Response Expert (on-premises)**
   - **KATA Sandbox**.
   - **Network Detection and Response (KATA)**.
7. Ajoutez les adresses IP pour lesquelles vous ne souhaitez pas utiliser de serveur proxy. Exemple : `1.2.3.4/24`, `1234::cdef/96`.
8. Enregistrez vos modifications.

Configuration des exclusions du serveur proxy via la ligne de commande

1. Pour ajouter des adresses pour lesquelles vous ne souhaitez pas utiliser de serveur proxy, exécutez la commande suivante :

   ```
   kesl-control --set-net-settings ProxyBypass=<address:port>
   ```
2. Pour contourner le serveur proxy pour les intégrations avec les solutions Kaspersky Detection and Response, exécutez la commande suivante :

   ```
   kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
   <Yes|No>]
   ```

3. Pour vérifier les valeurs actuelles des paramètres réseau, exécutez la commande suivante :

```
kesl-control --get-net-settings
```

Symboles

Options de la commande

Paramètre	Description
`ProxyBypass`	Liste des adresses pour lesquelles un serveur proxy n'est pas utilisé. L'adresse est spécifiée au format `<address>[:<port>]`. Pour spécifier des adresses, vous pouvez utiliser des masques (symbole `*`) et des commentaires après le symbole `\`.
`ProxyBypassEdr`	Utiliser un serveur proxy lors de la connexion aux serveurs d'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises). Par défaut, le serveur proxy n'est pas utilisé (`No`).
`ProxyBypassNdr`	Utiliser un serveur proxy lors de la connexion aux Serveurs permettant l'intégration de Kaspersky Network Detection and Response (KATA). Par défaut, le serveur proxy n'est pas utilisé (`No`).
`ProxyBypassSandbox`	Utiliser d'un serveur proxy lors de la connexion aux serveurs qui permettent l'interaction avec Sandbox. Par défaut, le serveur proxy n'est pas utilisé (`No`).

Comment l'application intercepte le trafic

L'application peut fonctionner dans l'un des deux modes d'interception du trafic réseau : eBPF ou iptables. Le mode iptables est sélectionné par défaut.

Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.

À propos de l'interception du trafic réseau via eBPF

En mode eBPF, l'application crée son propre espace de noms réseau distinct (network linux namespace), où elle redirige les paquets réseau à l'aide de programmes eBPF associés aux files d'attente `tc` (linux traffic control) des interfaces réseau locales. Le trafic réseau redirigé est ensuite analysé en fonction des tâches réseau actives, puis renvoyé à l'interface réseau d'origine.

Pour échanger des données entre espaces de noms réseau, des paires d'interfaces réseau virtuelles `veth` sont utilisées (chaque extrémité de la paire se trouve dans son propre espace de noms réseau) :

- La paire `kesl_in – kesl_worm_in` transmet le trafic réseau des connexions entrantes.
- La paire `kesl_out – kesl_worm_out` transmet le trafic réseau des connexions sortantes.

Par l'intermédiaire de ces paires d'interfaces, le trafic réseau est acheminé pour inspection de l'espace de noms par défaut vers l'espace de noms créé par l'application, puis renvoyé après analyse.

Le trafic réseau atteint ces interfaces depuis d'autres interfaces réseau du système uniquement si l'application est en cours d'exécution et que l'interception réseau est activée. Ils ne peuvent pas être utilisés pour transférer des données sur un réseau entre des appareils distants.

À propos de l'interception du trafic réseau via iptables

En mode iptables, l'interception est effectuée à l'aide du mécanisme du noyau tproxy.

Les règles correspondantes sont créées dans la chaîne PREROUTING de la table mangle afin de transférer le trafic vers un port spécial ouvert par l'application. L'application ajoute également des règles supplémentaires à différentes tables du pare-feu du système d'exploitation afin de transférer les paquets vers tproxy. L'intercepteur réseau de l'application se trouve entre le client et le serveur, établit une connexion distincte avec chacun d'eux, puis analyse et transmet le trafic entre eux.

Les connexions entrantes et sortantes interceptées sont marquées par des étiquettes distinctes, que vous pouvez modifier dans le fichier de configuration kesl.ini.

Pour les connexions sortantes, des règles de routage supplémentaires sont ajoutées afin de rediriger le trafic sortant pour les ports interceptés vers l'interface de bouclage dans tproxy.

Sélection du mode d'interception du trafic

Comment sélectionner un mode d'interception du trafic réseau dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Sous **Mode d'interception du trafic**, sélectionnez un mode d'interception du trafic pour l'application :
   - **iptables**. Sélectionné par défaut. L'application utilise l'outil iptables pour intercepter le trafic.
   - **eBPF**. L'application utilise la technologie eBPF pour intercepter le trafic.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner un mode d'interception du trafic réseau dans la ligne de commande

1. Exécutez la commande:

   ```
   kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
   ```

2. Pour vérifier les valeurs actuelles des paramètres réseau, exécutez la commande suivante :

   ```
   kesl-control --get-net-setting
   ```

Considérations particulières et limitations

- Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.
- Si l'application ne peut pas utiliser le mode eBPF pour intercepter le trafic réseau, le mode iptables est utilisé à la place.

Configuration de la stratégie de validation des certificats

Les paramètres d'analyse du trafic réseau sont utilisés dans le fonctionnement des modules Protection contre les menaces Internet, Protection contre les menaces réseau, Protection contre les menaces par emails et Contrôle Internet.

Par défaut, la Protection contre les menaces Internet déchiffre et analyse le trafic réseau transmis via des connexions chiffrées. Pour ce faire, l'application valide l'intégralité de la chaîne de certificats.

La stratégie de validation des certificats inclut les paramètres suivants :

- Méthode de validation (localement ou via Internet)
- Accès aux sites Internet avec un certificat non fiable
- Accès aux sites Internet avec une erreur de validation du certificat

Si l'appareil ne dispose pas d'une connexion directe à Internet, vous pouvez sélectionner la méthode de validation locale des certificats.

Par défaut, l'application autorise l'établissement d'une connexion réseau à un domaine doté d'un certificat non approuvé. L'application affiche une page HTML avec un avertissement et des informations sur la raison pour laquelle il n'est pas recommandé de visiter le domaine concerné (cf. ill. ci-dessous). Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé.

Si une application ou un service tiers établit une connexion avec un domaine présentant un certificat non fiable, l'application crée son propre certificat pour analyser le trafic. Le nouveau certificat porte l'état *Douteux*. Cette mesure est nécessaire pour avertir l'application tierce de la connexion douteuse, car la page HTML ne peut pas être affichée dans ce cas, et la connexion peut être établie en arrière-plan.

La validation du certificat peut se terminer par une erreur. Par exemple, lors de l'utilisation d'un stockage dans le cloud ou de la validation de certificats auto-signés. Par défaut, l'application ajoute les noms de domaine de ces sites Internet aux exclusions et ne contrôle pas le trafic réseau chiffré lors de la visite de ce domaine. L'application génère également un événement pour signaler l'erreur d'analyse de la connexion chiffrée.

Vous pouvez consulter la liste des domaines contenant des erreurs d'analyse des connexions chiffrées uniquement dans l'interface locale de l'application.

Configuration de la stratégie de validation des certificats dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux → Paramètres du réseau**.
5. Dans la section **Analyse des connexions chiffrées**, assurez-vous que le commutateur est en position **Analyse des connexions chiffrées ACTIVÉE**.

   Si le commutateur est désactivé, Kaspersky Endpoint Security n'a pas accès au contenu des sites Internet dont l'adresse commence par `https://`.
6. Suivez le lien **Paramètres** et configurez la stratégie de validation des certificats :

   - **Accès à un domaine doté d'un certificat douteux**. Action lors de l'utilisation d'un certificat douteux
     - **Autoriser la connexion**. L'application autorise les connexions à un domaine doté d'un certificat non approuvé. L'application affiche une page HTML avec un avertissement et des informations sur la raison pour laquelle il n'est pas recommandé de visiter le domaine concerné (cf. ill. ci-dessous). Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé.
     - **Bloquer la connexion**. Lors de l'accès à un domaine avec un certificat non fiable, Kaspersky Endpoint Security bloque la connexion réseau et affiche une page HTML qui indique la raison pour laquelle ce domaine est bloqué.
   - **Accès à un domaine présentant une erreur d'analyse des connexions chiffrées**. Action en cas d'erreur d'analyse d'une connexion chiffrée :
     - **Autoriser et ajouter le domaine aux exclusions**. Lorsqu'une erreur d'analyse d'une connexion chiffrée se produit, l'application ajoute le domaine à l'origine de l'erreur à la liste des exclusions et ne surveille pas le trafic réseau chiffré lors de la visite de ce domaine.
     - **Bloquer la connexion**. Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée.
   - **Stratégie de vérification du certificat**. Méthode utilisée par l'application pour valider les certificats :
     - **Vérification complète**. L'application utilise Internet pour vérifier et télécharger les chaînes manquantes nécessaires à la validation d'un certificat.
     - **Vérification locale**. L'application valide le certificat localement sur l'ordinateur.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration d'une stratégie de validation des certificats via la ligne de commande

1. Pour activer l'analyse des connexions chiffrées, exécutez la commande suivante :

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. Pour sélectionner une méthode de validation des certificats, exécutez la commande suivante :

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. Pour sélectionner l'action à effectuer lorsqu'un certificat non fiable est détecté, exécutez la commande suivante :

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. Pour sélectionner l'action à effectuer lorsqu'une erreur se produit lors de l'analyse d'une connexion chiffrée, exécutez la commande suivante :

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. Pour vérifier les valeurs actuelles des paramètres réseau, exécutez la commande suivante :

```
kesl-control --get-net-setting
```

Symboles

Options de la commande

Paramètre	Description
`EncryptedConnectionsScan`	Mode d'analyse des connexions chiffrées : `Yes` (par défaut). L'analyse des connexions chiffrées est activée. `No`. L'analyse des connexions chiffrées est désactivée.
`CertificateVerificationPolicy`	Stratégie de validation des certificats : `FullCheck` (par défaut). L'application utilise Internet pour vérifier et télécharger les chaînes manquantes nécessaires à la validation d'un certificat. `LocalCheck`. L'application valide le certificat localement sur l'ordinateur.
`UntrustedCertificateAction`	Action lors de l'utilisation d'un certificat douteux `Allow` (par défaut). L'application autorise les connexions à un domaine doté d'un certificat non approuvé. L'application affiche une page HTML avec un avertissement et des informations sur la raison pour laquelle il n'est pas recommandé de visiter le domaine concerné (cf. ill. ci-dessous). Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé. `Block`. Kaspersky Endpoint Security bloque l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. Lors de l'accès à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui indique la raison pour laquelle l'accès à ce domaine est bloqué.
`EncryptedConnectionsScanErrorAction`	Action en cas d'erreur d'analyse d'une connexion chiffrée : `AddToAutoExclusions` (par défaut). Lorsqu'une erreur d'analyse d'une connexion chiffrée se produit, l'application ajoute le domaine à l'origine de l'erreur à la liste des exclusions et ne surveille pas le trafic réseau chiffré lors de la visite de ce domaine. `Disconnect`. Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée.

Configuration des ports surveillés

Pendant l'exécution de Kaspersky Endpoint Security, le module Protection contre les menaces réseau surveille les données transmises via certains ports réseau. La liste des ports réseau surveillés par l'application est configurée conformément aux recommandations des experts de Kaspersky.

Les modules Détection comportementale et Protection contre les Exploits surveillent également les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus.

Vous pouvez configurer les ports que l'application doit surveiller :

- **Contrôler tous les ports réseau**. Mode de surveillance des ports réseau dans lequel l'application surveille les flux de données passant par tous les ports réseau ouverts de l'ordinateur.

  La spécification de cette valeur peut augmenter considérablement la charge d'un système d'exploitation.

- **Surveiller uniquement les ports réseau sélectionnés**. Dans ce mode de surveillance des ports réseau, les modules de la protection surveillent les ports sélectionnés de l'ordinateur ainsi que l'activité réseau des applications sélectionnées.

Si vous souhaitez intercepter les connexions réseau vers un serveur NFS, vous devez vous assurer que le serveur NFS est démarré avec l'option `insecure` (afin qu'il accepte les connexions provenant de ports situés en dehors de la plage 1-1024), sinon le serveur NFS peut rejeter ces connexions.

Configuration des ports surveillés dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Sous **Ports contrôlés**, sélectionnez le mode de surveillance des ports par l'application :
   - **Contrôler tous les ports réseau**.
   - **Surveiller uniquement les ports réseau sélectionnés** (valeur par défaut).
6. Si vous avez sélectionné l'option **Surveiller uniquement les ports réseau sélectionnés**, configurez la liste des ports à surveiller :
   a. Cliquez sur le lien **Ports surveillés**.
   b. Modifiez la liste des ports surveillés.

   Pour que la Protection contre les menaces par emails fonctionne, les ports réseau 25, 110, 143, 465, 587, 993 et 995 doivent être surveillés dans les paramètres réseau. Ces ports sont ajoutés par défaut à la liste des ports surveillés. Leur suppression de la liste peut perturber le fonctionnement du module.
7. Enregistrez vos modifications.

Configuration des ports surveillés via la ligne de commande

1. Pour sélectionner un mode de surveillance des ports, exécutez la commande suivante :

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
   ```

2. Si vous avez choisi de surveiller uniquement les ports sélectionnés (`MonitorNetworkPorts=Selected`), indiquez la liste des ports à surveiller :

   ```
   kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
   ```

   Pour supprimer un port de la liste de surveillance, modifiez la liste à l'aide d'un fichier de configuration.

3. Pour vérifier les valeurs actuelles des paramètres réseau, exécutez la commande suivante :

   ```
   kesl-control --get-net-settings
   ```

Symboles

Options de la commande

Paramètre	Description
`MonitorNetworkPorts`	`Selected` (valeur par défaut) : surveille uniquement les ports réseau spécifiés dans la section `[[NetworkPorts.item_#]` (voir ci-dessous). `All` : surveille tous les ports réseau. La spécification de cette valeur peut augmenter considérablement la charge d'un système d'exploitation.
`PortName`	Description du port réseau.
`Port`	Numéros de port réseau à surveiller par l'application. Valeurs possibles : `1 – 65535`. Pour que la Protection contre les menaces par emails fonctionne, les ports réseau 25, 110, 143, 465, 587, 993 et 995 doivent être surveillés dans les paramètres réseau. Ces ports sont ajoutés par défaut à la liste des ports surveillés. Leur suppression de la liste peut perturber le fonctionnement du module.

Exclusions à l'interception du trafic par le système d'exploitation

Dans les paramètres de l'application Kaspersky Endpoint Security, vous pouvez configurer des exclusions de l'interception du trafic en fonction de sa direction, de l'adresse IP et du port de destination. Si ces exclusions ne permettent pas de résoudre un conflit de communication réseau entre Kaspersky Endpoint Security et les applications client, vous pouvez utiliser la chaîne de règles spéciale kesl_bypass.

Cette chaîne est une liste de règles que Kaspersky Endpoint Security crée dans le tableau mangle du pare-feu du système d'exploitation (iptables/ip6tables). Les règles de la chaîne kesl_bypass permettent d'empêcher l'interception du trafic par l'application Kaspersky Endpoint Security. La chaîne kesl_bypass est ajoutée en premier lors du traitement des paquets réseau ; par conséquent, les règles kesl_bypass sont traitées avant toutes les autres règles iptables.

Contrairement aux exclusions, que vous pouvez configurer dans les paramètres de Kaspersky Endpoint Security, la chaîne kesl_bypass vous permet de configurer des exclusions non seulement par direction du trafic, adresse IP et port de destination, mais aussi en utilisant d'autres paramètres de connexion.

La modification des règles de la chaîne kesl_bypass s'opère à l'aide des outils du système d'exploitation.

Par exemple, vous pouvez ajouter une règle à la chaîne kesl_bypass en exécutant la commande suivante :

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

Cette règle empêche Kaspersky Endpoint Security d'intercepter le trafic HTTP entrant et sortant sur le port 80 et pour toute adresse IP. Cela permet d'éviter d'éventuels conflits avec les services web de confiance.

Si des règles d'exclusion de trafic sont configurées dans la chaîne, elles affectent le fonctionnement des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet.

Lors de la suppression de l'application, la chaîne de règles kesl_bypass dans iptables et ip6tables est supprimée uniquement si elle était vide.

Interception des opérations sur les fichiers

Le mode d'interception des opérations sur les fichiers affecte les modules Protection contre les fichiers malicieux et Contrôle des appareils, l'action Prévention de l'exécution des objets et la tâche Analyse des disques amovibles.

Si le mode de blocage de l'interception des opérations sur les fichiers est activé

- Une application peut bloquer l'accès aux fichiers analysés par le module Protection contre les fichiers malicieux pendant l'analyse. Si l'analyse ne détecte aucune menace dans le fichier, l'application autorise l'accès au fichier. Lorsque des objets infectés sont détectés, l'application exécute les actions définies dans le paramètre **Actions en cas de détection d'une menace** (`ActionOnThreat`) du module Protection contre les fichiers malicieux.

- Une application peut bloquer l'accès aux fichiers sur un appareil tandis que le Contrôle des appareils détermine si l'accès à l'appareil peut être accordé. L'application autorise l'accès aux fichiers si suite à une analyse, le Contrôle des appareils autorise l'accès à l'appareil contenant les fichiers.

- L'application peut bloquer des fichiers sur l'appareil pendant que la Prévention de l'exécution des objets détermine si ces fichiers peuvent être exécutés. L'application autorise l'exécution des fichiers si, à l'issue de l'analyse, la Prévention de l'exécution des objets permet leur exécution.

- L'application peut bloquer l'accès aux fichiers du disque amovible pendant l'analyse. Si l'analyse ne détecte aucune menace dans le fichier, l'application autorise l'accès au fichier. Lorsque des objets infectés sont détectés, l'application exécute les actions définies dans le paramètre **Actions en cas de détection d'une menace** (`ActionOnThreat`) du module Protection contre les fichiers malicieux.

Si le mode de blocage de l'interception des opérations sur les fichiers est désactivé

- Le module Protection contre les fichiers malicieux fonctionne en mode Informer quel que soit le mode de fonctionnement sélectionné et autorise l'accès aux fichiers en effectuant l'analyse de manière asynchrone.

- Le module Contrôle des appareils fonctionne en mode Informer, quel que soit le mode de fonctionnement sélectionné, et autorise toujours l'accès aux appareils.

- L'action Prévention de l'exécution des objets fonctionne en mode Informer, quel que soit le mode de fonctionnement sélectionné, et autorise toujours l'exécution des objets.
- L'application autorise toujours l'accès aux fichiers du disque amovible et effectue l'analyse de manière asynchrone.

Ce mode d'interception des opérations sur les fichiers a moins d'impact sur les performances du système, mais les menaces détectées dans les fichiers ne seront alors ni désinfectées ni supprimées. Cela peut se produire si, pendant une analyse, le processus associé au fichier parvient, par exemple, à le renommer avant que l'application ne détermine son statut. Vous pouvez exécuter la tâche Analyse des logiciels malveillants pour traiter ces menaces ultérieurement.

Par défaut, le mode de blocage lors de l'interception des opérations sur les fichiers est activé.

Configuration du mode d'interception des opérations sur les fichiers dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de détection**.
5. Dans la section **Mode d'interception des opérations sur les fichiers**, décochez ou cochez la case **Bloquer l'accès aux fichiers pendant les analyses**. La case est cochée par défaut.
6. Enregistrez vos modifications.

Configuration du mode d'interception des opérations sur les fichiers en ligne de commande

Sur la ligne de commande, vous pouvez configurer la manière dont les opérations sur les fichiers sont interceptées à l'aide du paramètre `FileBlockDuringScan` dans les paramètres généraux de l'application.

Pour sélectionner le mode d'interception des opérations sur les fichiers, exécutez la commande suivante :

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

Symboles

Options de la commande

Paramètre	Description
`FileBlockDuringScan`	`Yes` (valeur par défaut) pour bloquer l'accès aux fichiers pendant leur analyse par les modules Protection contre les fichiers malicieux et Contrôle des appareils, l'action Prévention de l'exécution et la tâche Analyse des disques amovibles. `No` : ne pas bloquer l'accès aux fichiers lors de l'analyse. L'accès à n'importe quel fichier est autorisé, la vérification est effectuée en mode asynchrone.

Configuration des paramètres d'interception des événements système

Vous pouvez choisir un mécanisme d'interception des événements système dans Web Console, sur la ligne de commande ou dans la Console d'administration.

Vous pouvez gérer les paramètres d'interception des événements système uniquement sur les appareils dont le système d'exploitation prend en charge la technologie fanotify.

La configuration de l'interception des événements système n'est pas disponible pour les appareils dotés d'un processeur Elbrus.

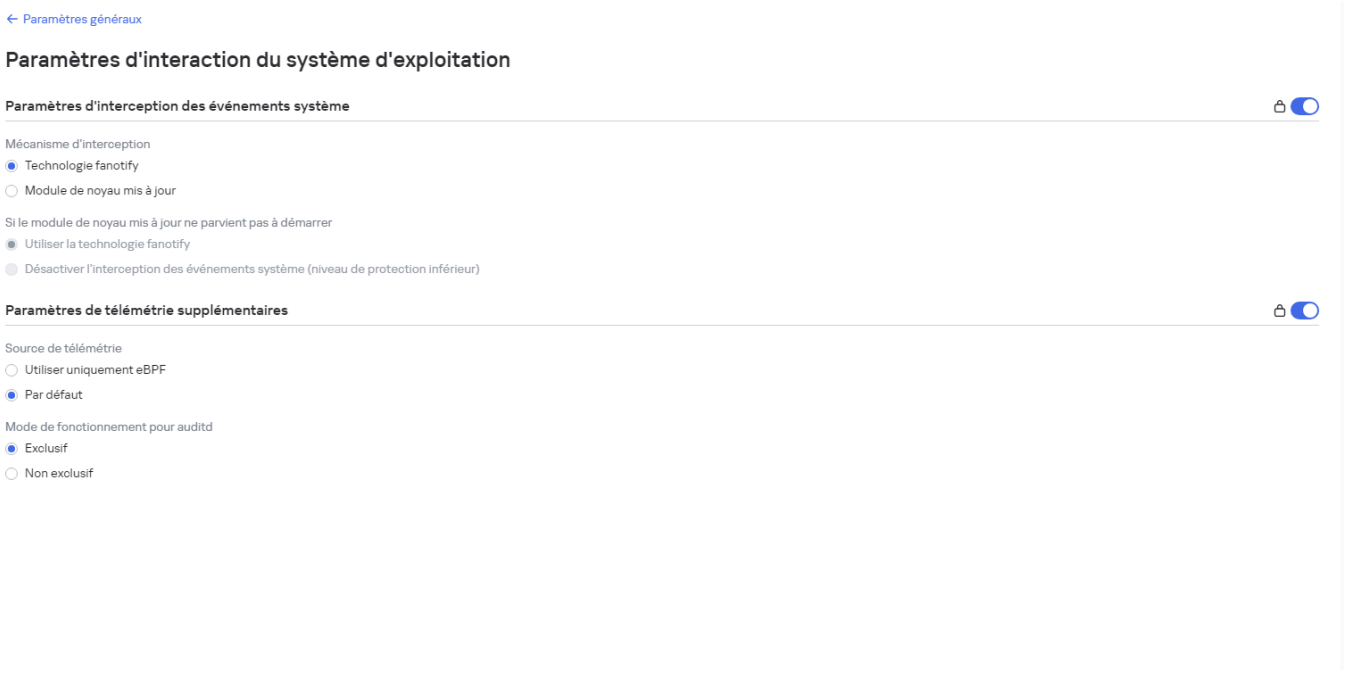
Configuration du mécanisme d'interception des événements système dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Paramètres généraux** → **Paramètres d'interaction du système d'exploitation**.

5. Sous **Paramètres d'interception des événements système**, sélectionnez un mécanisme d'interception des événements système :

   - **Technologie fanotify**.
   - **Module de noyau mis à jour**. Si cette option est sélectionnée, sélectionnez l'action que l'application exécutera si le module de noyau mis à jour ne parvient pas à démarrer :
     - **Utiliser la technologie fanotify**.
     - **Désactiver l'interception des événements système (niveau de protection inférieur)**.



Paramètres d'interaction avec le système d'exploitation

Configuration du mécanisme d'interception des événements système sur la ligne de commande

1. Pour sélectionner un mécanisme d'interception des événements système, exécutez la commande suivante :

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. Pour définir l'action que l'application exécute si le module de noyau mis à jour ne parvient pas à démarrer, exécutez la commande suivante :

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. Pour que l'application redémarre lorsque le module de noyau mis à jour ne parvient pas à démarrer, exécutez la commande suivante :

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. Pour vérifier les paramètres actuels de l'application, exécutez la commande suivante :

```
kesl-control --get-app-settings [--json]
```

Symboles

Options de la commande

Paramètre	Description
`InterceptorMode`	`UseFanotify` (valeur par défaut) : utiliser la technologie fanotify pour intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.
`InterceptorFallbackStrategy`	`FallbackToFanotify` (valeur par défaut) : passer à l'utilisation de la technologie fanotify pour intercepter les événements système. `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.
`InterceptorApplyStrategy`	`RestartServiceAutomatically` : redémarrer automatiquement l'application pour exécuter le module du noyau à actualiser. Nous vous recommandons d'utiliser ce paramètre. `RestartServiceManually` (valeur par défaut) : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur.

L'application peut utiliser le mécanisme d'interception basé sur le module de noyau mis à jour si le système d'exploitation satisfait aux exigences relatives à l'installation du module de noyau mis à jour.

Si vous sélectionnez le mécanisme d'interception basé sur le module de noyau mis à jour, vous pouvez configurer le comportement de l'application si une erreur se produit lors du démarrage du module du noyau mis à jour et que le module ne démarre pas. Dans ce cas, l'application peut passer à l'utilisation de la technologie fanotify pour intercepter les événements système ou désactiver l'interception des événements système.

Si le module de noyau mis à jour n'a pas pu être installé lors de l'installation de l'application, vous pouvez l'installer ultérieurement lorsque la prise en charge de votre système d'exploitation sera disponible. Pour ce faire, procédez comme suit :

1. Exécutez la mise à jour des bases et des modules de l'application. Le module de noyau mis à jour est installé dans le cadre d'une mise à jour.
2. Sélectionnez le mécanisme d'interception basé sur un module de noyau mis à jour.

Une application peut passer à l'utilisation d'un module de noyau mis à jour dans les situations suivantes :

- Si vous avez modifié le mécanisme d'interception des événements système dans les paramètres de l'application vers un module de noyau mis à jour.
- Si sur un appareil où le module de noyau mis à jour n'était pas en cours d'exécution, des mises à jour ont été reçues pendant la mise à jour des bases de l'application et des modules qui fournissent la prise en charge du module de noyau mis à jour.

Informations sur l'état du module de noyau mis à jour

Les informations sur l'état et la disponibilité du module de noyau mis à jour sont affichées sous forme d'états :

- **Démarré** signifie que le module est installé et en cours d'exécution.
- **Arrêté** signifie que le module est installé, mais n'est pas en cours d'exécution.

- **Non disponible** signifie que le module n'est pas pris en charge sur l'appareil.
- **Erreur de fonctionnement** signifie qu'une erreur s'est produite lors du démarrage du module et que le module n'est pas en cours d'exécution.

Vous pouvez consulter l'état du module de noyau mis à jour sur l'appareil dans Web Console et sur la ligne de commande.

Consultation de l'état du module de noyau mis à jour dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs → Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.
5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.
6. Consultez l'état du module fonctionnel **Module de noyau mis à jour**.

Consultation de l'état du module de noyau mis à jour sur la ligne de commande

Pour consulter l'état du module de noyau mis à jour, exécutez la commande suivante :

```
kesl-control --app-info [--json]
```

où `--json` signifie que les données sont affichées au format JSON. Si vous ne spécifiez pas la clé `--json`, les paramètres seront affichés dans la console.

Mode « Sécurisé » lors de l'utilisation d'un module de noyau mis à jour

Si l'application est instable lors de l'utilisation du module de noyau mis à jour, après avoir atteint le nombre maximal spécifié d'arrêts anormaux, l'application bascule automatiquement en mode de fonctionnement « sécurisé » (`SafeMode=yes` est défini dans le fichier de configuration kesl.ini). Par défaut, l'application passe en mode « sécurisé » après trois arrêts anormaux. Le nombre maximal d'arrêts anormaux de l'application est configuré dans le paramètre `PanicThreshold` du fichier de configuration kesl.ini.

Si l'application s'exécute en mode « sécurisé », le module de noyau mis à jour n'est pas lancé et l'application passe à l'utilisation de la technologie fanotify pour intercepter les événements système. L'application envoie le tag `UpdatableKernelModule=Error` à Kaspersky Security Center.

Pour continuer à utiliser le module de noyau mis à jour après avoir résolu les problèmes de l'application, vous devez désactiver le mode de fonctionnement « sécurisé ».

Désactivation du mode de fonctionnement sécurisé de l'application sur la ligne de commande

1. Ouvrez le fichier /var/opt/kaspersky/kesl/common/kesl.ini pour le modifier.
2. Dans la section `[General]`, définissez la valeur du paramètre `SafeMode=no`.
3. Redémarrez Kaspersky Endpoint Security :

```
systemctl restart kesl
```

Le mode de fonctionnement sécurisé est désactivé.

Configuration des paramètres avancés de la télémétrie

Vous pouvez configurer les paramètres avancés suivants pour la collecte de télémétrie envoyée aux solutions Detection and Response lors de leur intégration :

- Source de la télémétrie. La collecte de télémétrie peut être réalisée à l'aide d'eBPF et du service auditd, ou d'eBPF seul.
- Mode d'utilisation du service auditd. Kaspersky Endpoint Security peut utiliser le service auditd en mode exclusif ou en mode multidiffusion.

Comment configurer des paramètres de télémétrie supplémentaires dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres d'interaction du système d'exploitation**.
5. Sous **Paramètres de télémétrie**, spécifiez la source utilisée par Kaspersky Endpoint Security pour collecter la télémétrie :

   - **Utiliser eBPF uniquement** : utiliser la technologie eBPF seule pour la collecte de télémétrie.

     Si l'option **Utiliser uniquement eBPF** est sélectionnée, la télémétrie des solutions Detection and Response peut présenter des limitations.

   - **Par défaut** signifie que la technologie eBPF et le service auditd sont utilisés pour collecter la télémétrie.

6. Spécifiez également le mode d'utilisation du service auditd :

   - **Exclusif** signifie que Kaspersky Endpoint Security utilise le service auditd en mode exclusif.
   - **Multidiffusion** signifie que le service auditd est utilisé en mode multidiffusion.

   > Ce paramètre s'applique uniquement si le paramètre **Source de télémétrie** est défini sur **Par défaut**.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer des paramètres de télémétrie supplémentaires à partir de la ligne de commande

À partir de la ligne de commande, vous pouvez gérer les paramètres de télémétrie supplémentaires à l'aide des paramètres `TelemetrySource` et `UseTelemetryMonopolyMode` de la tâche prédéfinie Behavior_Detection.

1. Pour activer la source de télémétrie, exécutez la commande suivante :

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. Pour sélectionner un mode pour le service auditd, exécutez la commande suivante :

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

Symboles

Options de la commande

Paramètre	Description
`TelemetrySource`	`Default` (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie. `OnlyEBPF` : utiliser uniquement la technologie eBPF pour la collecte de télémétrie.
`UseTelemetryMonopolyMode`	`True` (valeur par défaut) : Kaspersky Endpoint Security utilise le service auditd en mode exclusif. `False` signifie que le service auditd est utilisé en mode multidiffusion. Le paramètre `UseTelemetryMonopolyMode` est appliqué uniquement si le paramètre `TelemetrySource` est défini sur `Default`.

Sauvegarde

Si, lors de l'analyse d'un appareil protégé, Kaspersky Endpoint Security détecte un code malveillant dans un fichier, l'application peut bloquer le fichier, lui attribuer l'état *Infecté*, et placer une copie dans la sauvegarde et tenter de désinfecter le fichier.

La *sauvegarde* est un stockage des copies de sauvegarde des fichiers qui ont été supprimés ou modifiés pendant la désinfection. La *copie de sauvegarde* est une copie d'un fichier créée avant que le fichier ne soit désinfecté ou supprimé. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations importantes devenues totalement ou partiellement inaccessibles suite au traitement, vous pouvez tenter de restaurer le fichier à partir d'une copie de sauvegarde de celui-ci.

La restauration d'objets infectés peut infecter l'appareil.

Les fichiers sauvegardés dans la sauvegarde peuvent contenir des données personnelles. Pour accéder aux objets de la sauvegarde, les privilèges root sont requis.

Configuration des paramètres de la sauvegarde

Vous pouvez gérer les paramètres de la sauvegarde sur un appareil dans Web Console, dans la Console d'administration ou à l'aide de la ligne de commande. Vous pouvez configurer les paramètres suivants de la sauvegarde :

- **Durée de stockage des objets dans la sauvegarde.** Par défaut, les objets sont stockés pendant 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens de la sauvegarde.
- **Taille maximale de la sauvegarde.** Par défaut, la taille maximale suivante de la Sauvegarde est configurée :
  - 0 Mo si aucune stratégie n'est appliquée
  - 1024 Mo si une stratégie est appliquée

  Une fois que la Sauvegarde a atteint sa taille maximale, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens dans afin que le volume de la Sauvegarde ne dépasse plus la valeur maximale.
- **Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine** (ce paramètre est configurable uniquement à l'aide de la ligne de commande). Par défaut, le répertoire /var/opt/kaspersky/kesl/common/objects-backup/ est utilisé pour stocker les copies de sauvegarde des fichiers et les fichiers en quarantaine.

Comment configurer les paramètres de la sauvegarde dans Web Console

Pour gérer les paramètres de la sauvegarde dans les propriétés de la stratégie :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Paramètres généraux** → **Rapports et stockage**.

5. Dans la section **Sauvegarde**, configurez les paramètres suivants :

   - **Supprimer les objets après (jours)**. Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La case est cochée par défaut.

     Les valeurs valides sont de 0 à 10000.

   - **Limiter la taille de la Sauvegarde à (Mo)**. Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. La case est cochée par défaut.

     Les valeurs valides sont de 1 à 4000.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Pour gérer les paramètres de la sauvegarde dans les propriétés de l'appareil administré :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des actifs** → **Actifs (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour sélectionner un groupe imbriqué, cliquez sur le bouton **Afficher la hiérarchie** dans la partie supérieure de la fenêtre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Cliquez sur le nom d'un appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Sélectionnez Kaspersky Endpoint Security

6. Accédez à **Paramètres de l'application** → **Paramètres de stockage**.

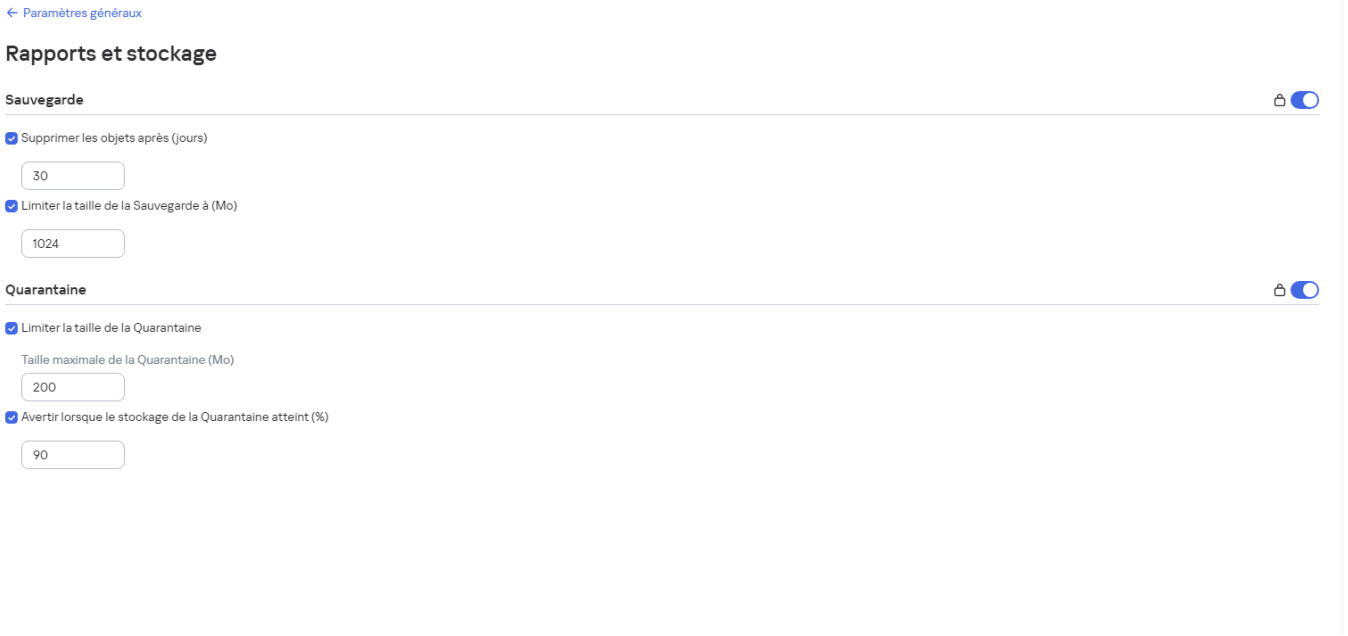
   - **Supprimer les objets après (jours)**. Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La case est cochée par défaut.

     Les valeurs valides sont de 1 à 10000.

   - **Limiter la taille de la Sauvegarde à (Mo)**. Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. La case est cochée par défaut.

     Les valeurs valides sont de 1 à 4000.

7. Enregistrez vos modifications.



Rapports et stockage

Comment configurer la sauvegarde à l'aide de la ligne de commande

À partir de la ligne de commande, vous pouvez configurer les paramètres de la sauvegarde à l'aide des paramètres `BackupDaysToLive`, `BackupSizeLimit` et `QuarantineBackupFolder` dans les paramètres généraux de l'application.

1. Pour configurer la durée de conservation des objets dans la Sauvegarde, exécutez la commande suivante :

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. Pour configurer la taille maximale de la Sauvegarde, exécutez la commande suivante :

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. Pour configurer le répertoire dans lequel sont stockés les objets de la Sauvegarde et de la Quarantaine, exécutez la commande suivante :

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. Pour vérifier les paramètres actuels de l'application, exécutez la commande suivante :

```
kesl-control --get-app-settings
```

Options de la commande

Paramètre	Description
`BackupDaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Après une durée spécifiée, l'application supprime les fichiers de sauvegarde les plus anciens. Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.
`BackupSizeLimit`	Volume maximal de la sauvegarde (Mo). Quand la taille de la sauvegarde atteint la valeur maximale définie, l'application supprime les objets les plus anciens. Pour supprimer la limite sur la taille de la sauvegarde, spécifiez la valeur 0.

Paramètre	Description
`QuarantineBackupFolder`	Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine. Vous pouvez définir un répertoire autre que celui défini par défaut. Les répertoires de n'importe quel appareil peuvent être utilisés comme répertoire pour stocker des objets de sauvegarde et de quarantaine. Il est déconseillé de désigner des répertoires qui se trouvent sur des appareils à distance, par exemple des répertoires montés via les protocoles Samba et NFS. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut. Valeur par défaut : `/var/opt/kaspersky/kesl/common/objects-backup/` L'accès au répertoire par défaut requiert les privilèges root.

Afficher les objets de la sauvegarde

Une liste générale des fichiers placés dans la sauvegarde par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans Web Console et dans la Console d'administration (**Avancé** → **Stockages** → **Sauvegarde**).

Kaspersky Security Center ne copie pas les fichiers de la sauvegarde vers le Serveur d'administration ; tous les fichiers sont placés dans la sauvegarde sur les appareils protégés.

Comment consulter dans Web Console les informations sur les objets de la sauvegarde

1. Dans la fenêtre principale de Web Console, sélectionnez **Stockages** → **Sauvegardes de fichiers**.

   Cette action ouvre la liste des fichiers placés dans la Sauvegarde par les applications de Kaspersky sur les appareils clients. Kaspersky Security Center ne copie pas les fichiers de la sauvegarde vers le Serveur d'administration ; tous les fichiers sont placés dans la sauvegarde sur les appareils protégés.

2. Consulter les propriétés des fichiers dans le stockage de sauvegarde sur les appareils protégés :

   - **Nom du fichier.**
   - **État** :
     - *Avertissement*
     - *Probablement infecté*
     - *Ajouté par l'utilisateur*
     - *Faux positif*
     - *Désinfecté*
     - *Non infecté*
     - *Protégé par mot de passe*
     - *Supprimé*
     - *Doit être envoyé à Kaspersky*
   - **Nom de l'appareil**

- **Action exécutée** :
  - *Suppression*
  - *Désinfection*
  - *Analyse*
  - *Restauration*
- **Objet**
- **Placé dans le stockage**
- **Entrée ajoutée par**
- **Taille (octets)**
- **Dossier restauré**
- **Utilisateur du système d'exploitation**
- **Description**
- **Nom du Serveur d'administration virtuel**

Comment afficher des informations sur les objets de la Sauvegarde en ligne de commande

Pour afficher des informations sur les objets de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

Où :

- `<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtre, l'application affichera des informations sur tous les objets de la sauvegarde.
- `<objects number>` indique le nombre d'objets les plus récents du stockage à afficher. Si vous ne spécifiez pas la clé `-n`, l'application affichera les informations des 30 objets les plus récents. Pour afficher les informations de tous les objets, indiquez la valeur `0`.
- `--json` : afficher les données au format JSON.

La ligne `ObjectId` affichera l'identifiant numérique que l'application a attribué à l'objet lors de son placement dans la sauvegarde. Cet identifiant est utilisé pour effectuer des actions sur un objet, telles que la restauration ou la suppression d'un objet de la Sauvegarde.

Comment afficher des informations sur les objets de la Sauvegarde dans l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Sauvegarde**.

   La fenêtre **Sauvegarde** s'ouvre.

La fenêtre affiche les informations suivantes sur les objets de la sauvegarde :

- nom de l'objet
- chemin complet vers un objet
- date à laquelle un objet a été ajouté à la sauvegarde
- la date à laquelle l'objet a été supprimé de la sauvegarde (ce champ est affiché si une limite est fixée sur la durée de conservation des objets dans la sauvegarde)
- taille de l'objet

Restauration des objets depuis la sauvegarde

Le fichier mis dans la sauvegarde est restauré à son emplacement d'origine selon les paramètres spécifiés. L'étiquette de mandat (uniquement sur les appareils exécutant Astra Linux) et les attributs du fichier source (sauf les attributs immutable et append-only) sont conservés lors de la restauration.

Sur les appareils exécutant Astra Linux, la restauration d'un fichier à partir d'une sauvegarde se termine par une erreur si :

- L'étiquette de mandat du fichier est supérieure à l'étiquette de capacité du répertoire de destination.
- L'étiquette de mandat du fichier est inférieure à celle du répertoire de destination et l'indicateur ccnr n'est pas défini pour ce répertoire.
- Sur les appareils exécutant le système d'exploitation Astra Linux, en mode environnement logiciel fermé, vous ne pouvez restaurer un fichier que sous le compte sous lequel il a été placé dans la sauvegarde. Lors de la restauration d'un fichier, l'application crée un répertoire avec l'étiquette MAC 3 (indicateur cnnr).

Pour effectuer des actions avec les fichiers de la sauvegarde dans Kaspersky Security Center, vous devez activer le transfert de données sur les fichiers de la sauvegarde vers le Serveur d'administration.

La restauration d'objets infectés peut infecter l'appareil.

Comment restaurer des objets depuis la Sauvegarde dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Stockages → Sauvegardes de fichiers**.

   Cette action ouvre la liste des fichiers placés dans la Sauvegarde par les applications de Kaspersky sur les appareils clients. Kaspersky Security Center ne copie pas les fichiers de la sauvegarde vers le Serveur d'administration ; tous les fichiers sont placés dans la sauvegarde sur les appareils protégés.

2. Cochez les cases en regard des fichiers que vous souhaitez restaurer.

3. Cliquez sur **Restaurer**.

   Les objets de la Sauvegarde sur les appareils clients sont restaurés.

Comment restaurer des objets depuis la Sauvegarde en ligne de commande

Pour restaurer un objet sous son nom d'origine dans son emplacement d'origine, exécutez la commande suivante :

```
kesl-control -B --restore <object id>
```

Où `<object id>` est l'identifiant numérique que l'application a attribué à l'objet lors de son placement dans la Sauvegarde.

Pour restaurer un objet sous un nouveau nom dans le répertoire indiqué, exécutez la commande suivante :

```
kesl-control -B --restore <object id> --file <path to file>
```

Où `--file <path to file>` est le nouveau nom du fichier et le chemin d'accès au répertoire dans lequel vous souhaitez l'enregistrer. Si le répertoire indiqué n'existe pas, l'application le crée.

Sur les appareils exécutant le système d'exploitation Astra Linux, en mode environnement logiciel fermé, vous ne pouvez restaurer un fichier que sous le compte sous lequel il a été placé dans la sauvegarde.

Comment restaurer des objets depuis la Sauvegarde dans l'interface graphique

Pour restaurer des objets depuis la Sauvegarde dans leurs répertoires d'origine :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Sauvegarde**.

   La fenêtre **Sauvegarde** s'ouvre.

3. Sélectionnez les objets que vous souhaitez restaurer.

4. Cliquez sur **Restaurer**.

Les objets de la Sauvegarde sont restaurés et deviennent disponibles dans le répertoire d'origine.

Les informations sur la restauration et la suppression des objets sont enregistrées dans le journal des événements.

Suppression des objets de la sauvegarde

Une fois qu'un délai spécifié s'est écoulé ou que la taille maximale de la sauvegarde a été atteinte, l'application supprime automatiquement les copies de sauvegarde les plus anciennes des fichiers avec n'importe quel état de la sauvegarde.

Vous pouvez également supprimer vous-même la copie de sauvegarde du fichier restauré et non restauré.

Comment supprimer des objets de la Sauvegarde dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Stockages** → **Sauvegardes de fichiers**.

   Cette action ouvre la liste des fichiers placés dans la Sauvegarde par les applications de Kaspersky sur les appareils clients. Kaspersky Security Center ne copie pas les fichiers de la sauvegarde vers le Serveur d'administration ; tous les fichiers sont placés dans la sauvegarde sur les appareils protégés.

2. Cochez les cases en regard des fichiers que vous souhaitez supprimer.

3. Cliquez sur le bouton **Supprimer**.

Les objets de la Sauvegarde sur les appareils clients sont supprimés.

Comment supprimer des objets de la Sauvegarde en ligne de commande

Pour supprimer les objets sélectionnés de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

Où `<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête.

Exemples :

```
Supprimer l'objet ayant ID=15
```

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

```
Supprimer les objets dont le nom ou le chemin contient "test"
```

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

Pour supprimer tous les objets de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --mass-remove
```

Comment supprimer des objets de la Sauvegarde dans l'interface graphique

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Sauvegarde**.

   La fenêtre **Sauvegarde** s'ouvre.

3. Sélectionnez les objets que vous souhaitez supprimer.

4. Cliquez sur le bouton **Supprimer**.

Les objets de la Sauvegarde seront supprimés. Les objets supprimés ne peuvent être restaurés à l'avenir.

Les informations sur la restauration et la suppression des objets sont enregistrées dans le journal des événements.

Protection contre les menaces avancées et les attaques ciblées

Les solutions Kaspersky Detection and Response sont des systèmes de sécurité permettant de détecter les menaces avancées et les indicateurs d'attaque à différents niveaux de l'infrastructure d'une organisation. Les solutions de Detection and Response fournissent des informations sur les menaces détectées et vous permettent de gérer votre réponse aux détections.

Kaspersky Endpoint Security peut interagir avec les solutions de détection et de réponse suivantes de Kaspersky :

- Kaspersky Endpoint Detection and Response Expert (on-premises) sur Open Single Management Platform (OSMP). L'intégration est assurée par le module de l'application Kaspersky Endpoint Security, Endpoint Detection and Response Expert (on-premises) (ci-après également appelé *EDR Expert (on-premises)*).
- Kaspersky Endpoint Detection and Response Expert (cloud) sur Open Single Management Platform (OSMP). L'intégration est assurée par le module de l'application Kaspersky Endpoint Security, Endpoint Detection and Response Expert (cloud) (ci-après également appelé *EDR Expert (cloud)*).
- Les modules Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sont intégrés à Kaspersky Anti Targeted Attack Platform. L'intégration est assurée par les modules suivants de Kaspersky Endpoint Security :
  - Endpoint Detection and Response Expert (on-premises) (ci-après également appelé *EDR Expert (on-premises)*).
  - Network Detection and Response (KATA) (ci-après également *NDR (KATA)*).
- Sandbox sur Open Single Management Platform (OSMP) ou sur Kaspersky Anti Targeted Attack Platform. L'intégration est assurée par le module *Sandbox* de l'application Kaspersky Endpoint Security.
- Kaspersky Unified Monitoring and Analysis Platform.
- Kaspersky Endpoint Detection and Response Optimum. L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (ci-après également appelé *EDR Optimum*).
- Kaspersky Managed Detection and Response. L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Managed Detection and Response (ci-après également appelé *MDR*).

Fonctionnalités d'intégration des solutions Detection and Response

- Si vous utilisez Kaspersky Endpoint Security en mode EDR Agent, l'intégration est prise en charge uniquement avec Kaspersky Endpoint Detection and Response Expert (on-premises) sur Open Single Management Platform (OSMP) et avec les modules Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sur Kaspersky Anti Targeted Attack Platform.

- Lorsque Kaspersky Endpoint Security est intégré à Kaspersky Managed Detection and Response et à Kaspersky Anti Targeted Attack Platform, l'agent intégré peut consigner un grand nombre d'événements dans le journal systemd-journald. Si vous souhaitez désactiver la journalisation des événements d'audit dans le journal systemd-journald, désactivez le socket systemd-journald-audit et redémarrez le système d'exploitation.

  Désactiver le socket systemd-journald-audit

  ```
  systemctl stop systemd-journald-audit.socket
  systemctl disable systemd-journald-audit.socket
  systemctl mask systemd-journald-audit.socket
  ```

- Par défaut, sur le système d'exploitation SynthesisM-Client, la configuration du service auditd est bloquée contre les modifications, c'est-à-dire qu'elle est dans le mode de fonctionnement `enabled 2`. Pour que le module Détection comportementale fonctionne correctement lors de l'intégration de Kaspersky Endpoint Security avec les solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform, vous devez modifier le mode de fonctionnement auditd dans les fichiers de configuration en mode sans bloquer la configuration `enabled 1` et redémarrer le système d'exploitation.

- Les solutions Detection and Response peuvent ne pas fonctionner correctement sur les machines virtuelles créées à partir d'une image sur laquelle Kaspersky Endpoint Security for Linux est installé. Lors de l'intégration aux solutions Detection and Response, un identifiant unique (Sensor ID) de l'ordinateur est utilisé. L'application génère cet identifiant lors de l'installation initiale, et il est conservé même après la désinstallation de l'application. Lors du clonage d'une image, la machine virtuelle hérite du Sensor ID, ce qui peut conduire les solutions Detection and Response à identifier plusieurs machines virtuelles comme étant le même appareil.

  Recommandations relatives à la création d'une image de référence pour une intégration correcte avec MDR

  Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premises)

Actions de réponse

Lors de l'intégration avec les solutions Detection and Response, l'application Kaspersky Endpoint Security peut effectuer des actions de réponse visant à garantir les fonctions de sécurité. Les actions de réponse peuvent être générées côté solution Detection and Response et exécutées automatiquement sur les appareils équipés de Kaspersky Endpoint Security si cette fonction est activée dans les paramètres de la solution Detection and Response. Vous pouvez également configurer et exécuter manuellement les actions de réponse.

Les options de réponse varient en fonction de la solution Detection and Response avec laquelle l'application Kaspersky Endpoint Security est intégrée.

L'application Kaspersky Endpoint Security peut effectuer les actions de réponse suivantes :

- Isolation réseau d'un appareil.

Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response Expert (cloud), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, l'isolement du réseau est activé ou désactivé du côté de la solution Detection and Response correspondante. Vous pouvez désactiver manuellement l'isolement réseau d'un appareil.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, l'appareil peut être isolé du réseau automatiquement ou manuellement. Vous pouvez configurer les paramètres d'isolement du réseau et désactiver manuellement l'isolement du réseau pour votre appareil.

- Mettre un fichier en quarantaine.

  L'action est effectuée à l'aide de la tâche de mise des fichiers en quarantaine (Quarantine file).

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, un fichier peut être mis en quarantaine automatiquement suite à la détection d'indicateurs de compromission.

  Lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response, vous pouvez également mettre les fichiers en quarantaine manuellement.

- Restauration d'un fichier depuis la quarantaine.

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response Expert (cloud), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, l'action de réponse à la menace est générée du côté de la solution Detection and Response correspondante. Vous pouvez également effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

- Suppression d'un fichier de la quarantaine.

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response Expert (cloud), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, l'action de réponse à la menace est générée du côté de la solution Detection and Response correspondante. Vous pouvez également effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

- Récupération d'un fichier depuis la quarantaine.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response Expert (cloud) ou avec Kaspersky Endpoint Detection and Response (KATA), l'action de réponse à la menace est générée du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center.

- Réception d'un fichier depuis l'appareil.

  L'action est effectuée à l'aide de la tâche d'obtention du fichier depuis l'appareil (*Get file*). Par exemple, vous pouvez configurer pour recevoir un fichier journal des événements généré par un logiciel tiers.

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer des tâches pour recevoir des fichiers à partir des appareils dans Web Console.

- Suppression d'un fichier de l'appareil.

  L'action est effectuée à l'aide de la tâche de suppression du fichier de l'appareil (*Delete file*).

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response Expert (cloud) ou avec Kaspersky Endpoint Detection and Response (KATA), la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer des tâches de suppression des fichiers à partir des appareils dans Web Console.

- Lancer à distance un processus sur un appareil.

  L'action est effectuée à l'aide de la tâche d'exécution du processus (*Run application*). Par exemple, vous pouvez exécuter à distance un utilitaire qui crée un fichier de configuration de l'appareil, puis récupérer le fichier créé à l'aide de la tâche de réception d'un fichier depuis un appareil.

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer et exécuter des tâches de lancement des processus dans Web Console.

- Terminer à distance un processus sur un appareil.

  L'action est effectuée à l'aide de la tâche de fin du processus (*Kill process*). Par exemple, vous pouvez arrêter à distance l'utilitaire de test de vitesse Internet lancé à l'aide de la tâche de démarrage du processus.

  Lors de l'intégration avec Endpoint Detection and Response Expert (on-premises), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer et exécuter des tâches de terminaison des processus dans Web Console.

- Détecter les indicateurs de compromission (IOC) sur les appareils.

  Indicateur de compromission (Indicator of Compromise, IOC) est un ensemble de données sur un objet ou une activité qui indique un accès non autorisé à un appareil (compromission de données). Par exemple, un indicateur de compromission pourrait être un nombre élevé de tentatives de connexion échouées.

- Lancement de l'*analyse YARA*.

  Une *analyse YARA* est un processus au cours duquel Kaspersky Endpoint Security utilise des fichiers YARA pour rechercher des signatures d'activités malveillantes sur l'appareil. Les *fichiers YARA* sont des fichiers avec l'extension YARA ou YAR qui contiennent des règles YARA. Les *règles YARA* décrivent les signatures des attaques ciblées et des intrusions dans l'infrastructure informatique d'une organisation. Kaspersky Endpoint Security analyse les objets à l'aide de ces règles. Si une règle est détectée, l'analyseur signale une infection et consigne les détails correspondants dans le journal. L'analyse est effectuée de manière récursive sur les disques locaux. L'analyse des ressources réseau, connectées et cloud n'est pas prise en charge.

  La commande d'analyse YARA sur un appareil où Kaspersky Endpoint Security est installé est créée et exécutée du côté des solutions Kaspersky Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response Expert (cloud).

- Prévention de l'exécution

- Collecte de données forensiques.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response Expert (cloud), vous pouvez collecter des données numériques qui peuvent être utiles lors d'enquêtes sur des incidents liés à des cybercrimes et à des fuites de données.

Ceci est réalisé à l'aide des tâches suivantes :

- une tâche de collecte de données forensiques *Get forensics*, qui collecte les types d'informations suivants :
  - une liste de fichiers
  - une liste de processus
  - une liste de points de démarrage
- des tâches de génération de vidage mémoire (*Get memory dump*)
- des tâches de génération d'un vidage de mémoire du processus (*Get process memory dump*)
- des tâches d'image disque (*Get disk image*)

Les tâches sont créées et lancées du côté des solutions Kaspersky Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response Expert (cloud).

Trouver des indicateurs de compromission

Un *indicateur de compromission (IOC)* est un ensemble de données concernant un objet ou une activité qui indique un accès non autorisé à l'ordinateur (compromission des données). Par exemple, un indicateur de compromission pourrait être un nombre élevé de tentatives de connexion échouées. La tâche *Analyse IOC* permet de trouver des indicateurs de compromission sur l'ordinateur et de prendre des mesures de réponse aux menaces.

La fonctionnalité d'analyse IOC est disponible dans l'application Kaspersky Endpoint Security si l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.

  Dans ce cas, la recherche d'IOC est effectuée à l'aide de la tâche *Analyse IOC*.

- L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premises) est activé.

  Dans ce cas, l'analyse IOC est effectuée du côté de la solution correspondante.

Lors de l'exécution de la tâche Analyse IOC, l'analyse des termes IOC (propriétés de l'objet IOC, par exemple, somme de hachage du fichier) est effectuée uniquement dans l'espace de noms principal du système d'exploitation. La tâche *Analyse IOC* ne calcule pas les sommes de hachage des fichiers de plus de 200 Mo.

Pour rechercher des indicateurs de compromission, Kaspersky Endpoint Security utilise les fichiers IOC préparés par l'utilisateur. Si vous souhaitez ajouter manuellement un indicateur de compromission, veuillez consulter les exigences du fichier IOC. Si le fichier IOC ne répond pas aux exigences, l'application ne pourra pas l'utiliser.

Les identifiants de tous les fichiers IOC utilisés dans une seule tâche d'analyse IOC doivent être uniques. Si vous téléchargez plusieurs fichiers IOC avec les mêmes ID, l'application n'utilise qu'un seul de ces fichiers IOC. Les fichiers IOC restants seront automatiquement exclus.

Création d'une tâche Analyse IOC

Vous pouvez créer des tâches *Analyse IOC* manuellement :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

- À l'aide de l'Assistant de création d'une tâche.

- Localement via la ligne de commande.

Comment créer une tâche Analyse IOC dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux 12.5**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Analyse IOC**.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

   d. Sous **Appareils auxquels la tâche sera affectée**, sélectionnez la manière dont vous souhaitez définir la zone d'action de la tâche.

4. Sélectionnez les appareils selon la méthode de définition de la zone d'action de la tâche que vous préférez. Passez à l'étape suivante.

5. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

7. Sélectionnez l'onglet **Paramètres de l'application**.

8. Passez à la section **Analyse des menaces**.

9. Chargez les fichiers IOC pour rechercher des indicateurs de compromission.

Une fois les fichiers IOC chargés, l'application affiche un résumé des informations relatives au fichier, y compris la liste des indicateurs qui n'ont pas réussi la vérification. Après avoir téléchargé les fichiers IOC, vous pouvez modifier les fichiers manuellement dans l'éditeur intégré directement dans les propriétés de la tâche. Kaspersky Endpoint Security prend en charge l'édition des fichiers IOC conformes à la norme OpenIOC 1.1. Il n'est pas possible de modifier le contenu des fichiers IOC conformes à OpenIOC version 1.0.

Kaspersky Endpoint Security ajoute les fichiers IOC à la collection IOC. Le cas échéant, vous pouvez exclure temporairement les fichiers IOC de la zone d'action de la tâche.

Il n'est pas recommandé d'ajouter ou de supprimer des fichiers IOC une fois la tâche démarrée. Cela peut entraîner un affichage incorrect des résultats de l'analyse IOC pour les exécutions des tâches précédentes. Pour rechercher des indicateurs de compromission dans les nouveaux fichiers IOC, il est recommandé d'ajouter de nouvelles tâches.

10. Passez à la section **Paramètres d'analyse**.

11. Si nécessaire, configurez l'analyse IOC rétrospective.

    Analyse IOC rétrospective est un mode de la tâche *Analyse IOC* dans laquelle Kaspersky Endpoint Security recherche des indicateurs de compromission à l'aide des données pendant une certaine période. Ce mode est destiné à la recherche d'indicateurs de compromission à partir des données de télémétrie de l'ordinateur protégé, telles que l'activité réseau, les processus, les fichiers et d'autres données télémétriques. Kaspersky Endpoint Security analyse les données contenues dans les journaux du système d'exploitation et les journaux du navigateur sur l'ordinateur. L'analyse IOC rétrospective analyse les journaux des navigateurs suivants : Google Chrome, Mozilla Firefox, Microsoft Edge (version 79 ou ultérieure).

    a. Sous **Analyse IOC rétrospective**, accédez aux paramètres de recherche.

    b. Activez le commutateur **Analyse IOC rétrospective**.

    c. Définissez l'intervalle de temps pour les analyses IOC rétrospectives.

12. Sélectionnez les types de données (documents IOC) qui doivent être analysés dans le cadre de la tâche.

    Kaspersky Endpoint Security sélectionne automatiquement les types de données (documents IOC) pour la tâche *Analyse IOC* conformément au contenu des fichiers IOC chargés. Il est déconseillé de désélectionner les types de données.

    En outre, vous pouvez configurer les zones de recherche pour le type de données **Fichiers - FileItem**. Définissez une zone d'analyse IOC sur l'ordinateur à l'aide de zones prédéfinies.

13. Passez à la section **Paramètres de réponse**.

14. Sélectionnez le mode de fonctionnement de la tâche : **Alerter uniquement** ou **Alerter et répondre**.

15. Sélectionnez une action de réponse à appliquer lorsqu'un IOC est détecté :

    - **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security vérifie la mémoire du noyau, les processus en cours d'exécution et les secteurs de démarrage.

Zones critiques analysées par Kaspersky Endpoint Security

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession

- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- **Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer un objet, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où vous auriez besoin ultérieurement de restaurer l'objet. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.

  Si cette case est décochée, vous pouvez mettre le fichier en quarantaine manuellement après avoir exécuté la tâche manuellement. Si la tâche *Analyse IOC* détecte un fichier qui peut compromettre les données, vous pouvez mettre ce fichier en quarantaine directement à partir des résultats de l'analyse IOC (**Paramètres de l'application → Résultats de l'analyse IOC**). Kaspersky Endpoint Security lance alors l'Assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

- **Isoler l'appareil du réseau**. Si cette option est sélectionnée, Kaspersky Endpoint Security isole l'ordinateur du réseau afin d'empêcher la propagation de la menace. Vous pouvez configurer la durée de l'isolation dans les paramètres du module Endpoint Detection and Response.

  Si cette case est décochée, vous pouvez isoler l'ordinateur du réseau après avoir exécuté la tâche manuellement. Si la tâche *Analyse IOC* détecte un fichier qui peut compromettre les données, vous pouvez mettre ce fichier en quarantaine directement à partir des résultats de l'analyse IOC (**Paramètres de l'application → Résultats de l'analyse IOC**). Kaspersky Endpoint Security lance alors l'Assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

16. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.
17. Programmez l'exécution de la tâche.

    Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

18. Enregistrez vos modifications.
19. Cochez la case en regard de la tâche.
20. Cliquez sur **Démarrer**.

Vous pouvez consulter le résultat de la tâche *Analyse IOC* dans les propriétés de la tâche dans Web Console sous **Résultats de l'analyse IOC**. La période de conservation des résultats de l'analyse IOC est de 30 jours. Passé ce délai, Kaspersky Endpoint Security supprime automatiquement les anciens enregistrements.

Comment créer une tâche Analyse IOC en ligne de commande

Exécutez la commande :

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Symboles

Paramètre	Description
`--path`	Chemin d'accès au fichier IOC ou au répertoire contenant les fichiers IOC avec l'extension .IOC ou .XML, à utiliser pour effectuer l'analyse. Les *fichiers IOC* sont des fichiers contenant les ensembles d'indicateurs que l'application tente de faire correspondre pour compter une détection. Les fichiers IOC doivent être conformes standard OpenIOC. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces. Vous pouvez également spécifier les deux types de chemins (fichier et répertoire).
`--process`	Analyser les données du processus lors de l'analyse IOC (terme ProcessItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les processus en cours d'exécution sur l'ordinateur lors de l'analyse. Si le fichier IOC contient des termes IOC du document IOC ProcessItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données de processus uniquement si le document IOC ProcessItem est décrit dans le fichier IOC fourni pour l'analyse.
`--hint`	Analyser les données des fichiers lors de l'analyse IOC (termes ProcessItem et FileItem). Vous pouvez sélectionner un fichier d'une des manières suivantes : • `<full path to the executable file of the process>` : terme ProcessItem ; • `<full path to the file>` : terme FileItem.
`--arpentry`	Analyser les données relatives aux enregistrements de la table ARP lors de l'exécution de l'analyse IOC (terme ArpEntryItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le tableau ARP. Si le fichier IOC contient des termes du document IOC ArpEntryItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le tableau ARP uniquement si le document IOC ArpEntryItem est décrit dans le fichier IOC fourni pour l'analyse.
`--ports`	Analyser les données relatives aux ports ouverts à l'écoute lors de l'analyse IOC (terme PortItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le tableau des connexions actives sur l'appareil. Si le fichier IOC contient des termes du document IOC PortItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le tableau des connexions actives uniquement si le document IOC PortItem est décrit dans le fichier IOC fourni pour l'analyse.
`--system`	Analyser les données de l'environnement lors de l'analyse IOC (terme SystemInfoItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données de l'environnement. Si le fichier IOC contient des termes du document IOC SystemInfoItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données de l'environnement uniquement si le document IOC SystemInfoItem est décrit dans le fichier IOC fourni pour l'analyse.
`--files`	Analyser les données des fichiers lors de l'analyse IOC (terme FileItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données des fichiers. Si le fichier IOC contient des termes du document IOC FileItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données relatives aux fichiers uniquement si le document IOC FileItem est décrit dans le fichier IOC fourni pour l'analyse.
`--drives`	Définir la zone d'analyse IOC lors de l'analyse des données pour le document IOC FileItem. Vous pouvez définir les valeurs suivantes pour la zone d'analyse : • `<all>` pour toutes les zones d'actions de fichiers disponibles. • `<system>` pour les fichiers dans les dossiers où le système d'exploitation est installé. • `<critical>` pour les fichiers temporaires dans les dossiers de l'utilisateur et du système. • `<custom>` pour les fichiers dans les champs d'application définis par l'utilisateur (`/scope=<list of folders to scan>`). Si l'argument n'est pas indiqué, l'analyse est effectuée pour les zones critiques.
`--excludes`	Définir la zone d'exclusion lors de l'analyse des données pour le document IOC FileItem. Vous pouvez indiquer plusieurs chemins séparés par des espaces.
`--scope`	Zone d'analyse IOC définie par l'utilisateur lors de l'analyse des données pour le document IOC FileItem (`/drives=custom`). Vous pouvez indiquer plusieurs chemins séparés par des espaces.

Paramètre	Description
`--action`	Action effectuée lorsque des indicateurs de compromission sont détectés : • `Skip`. Si cette option est sélectionnée, Kaspersky Endpoint Security détecte uniquement les fichiers susceptibles de compromettre les données. • `QuarantineFile`. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer un objet, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où vous auriez besoin ultérieurement de restaurer l'objet. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine. • `IsolateHost`. Si cette option est sélectionnée, Kaspersky Endpoint Security isole l'ordinateur du réseau afin d'empêcher la propagation de la menace. • `ScanCriticalAreas`. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security vérifie la mémoire du noyau, les processus en cours d'exécution et les secteurs de démarrage.

Isolation réseau

Lorsqu'il est intégré aux solutions Detection and Response, un appareil peut être isolé du réseau dans le cadre d'une action de réponse aux menaces.

Caractéristiques de l'isolement du réseau

Une fois l'isolement du réseau activé, l'application interrompt toutes les connexions réseau TCP/IP actives et bloque toutes les nouvelles connexions réseau TCP/IP sur l'appareil, à l'exception des connexions suivantes :

- Connexions spécifiées dans les exclusions de l'isolement du réseau.
- Connexions initiées par les services de Kaspersky Endpoint Security.
- Connexions initiées par l'Agent d'administration de Kaspersky Security Center.
- connexions avec la SVM et le Serveur d'intégration si l'application est utilisée en mode Light Agent.
- Connexions à KSN (lorsqu'il est intégré à Kaspersky Managed Detection and Response).

L'isolement du réseau peut être appliqué lorsque l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premises) est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée et le module MDR est activé.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Detection and Response (KATA) et Kaspersky Managed Detection and Response, l'isolement réseau d'un appareil est activé ou désactivé, et les exclusions de l'isolement réseau sont configurées du côté de la solution Detection and Response. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises), l'aide de Kaspersky Anti Targeted Attack Platform ou l'aide de Kaspersky Managed Detection and Response. Si nécessaire, vous pouvez désactiver manuellement l'isolation réseau pour l'appareil :

- Dans les propriétés de l'appareil dans Web Console (uniquement en cas d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA))
- Dans la ligne de commande.

La désactivation manuelle de l'isolement du réseau est disponible, que l'intégration avec les solutions Detection and Response soit activée ou non, et que l'appareil soit couvert par une stratégie ou non.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, l'isolement du réseau peut être appliqué dans l'un des modes suivants :

- Mode automatique de l'isolement du réseau. L'appareil peut être isolé automatiquement du réseau suite à la détection d'indicateurs de compromission. Si, lors de la création et de la configuration des paramètres de la tâche *Analyse IOC* dans le groupe **Actions en cas de détection d'un IOC**, vous avez coché les cases **Appliquer les actions de réponse lorsqu'un IOC est détecté** et **Isoler l'appareil du réseau**, puis l'isolement du réseau est activé automatiquement lorsque l'application détecte des indicateurs de compromission.

  Vous pouvez configurer les paramètres d'isolement du réseau suivants en mode automatique :

  - Modifier la période de temps après laquelle l'isolement du réseau est automatiquement désactivé.
  - Configurer les exclusions de l'isolement du réseau pour les appareils isolés automatiquement.

  > Si un appareil isolé en mode automatique est soumis à une stratégie, les paramètres spécifiés dans la stratégie sont appliqués. Si la stratégie n'est pas appliquée, les paramètres spécifiés dans les propriétés de l'appareil sont appliqués.

- Mode manuel de l'isolement du réseau. L'appareil peut être isolé du réseau pendant que la menace détectée est étudiée. Vous pouvez activer manuellement l'isolement réseau pour un appareil dans la fenêtre des détails de l'alerte et dans les propriétés de l'appareil dans Web Console.

  Vous pouvez configurer les paramètres d'isolement du réseau suivants en mode manuel :

  - Modifier la période de temps après laquelle l'isolement du réseau est automatiquement désactivé.
  - Configurer les exclusions de l'isolement du réseau pour les appareils isolés manuellement.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez désactiver manuellement l'isolement réseau d'un appareil dans les propriétés de l'appareil dans Web Console et dans la ligne de commande.

Vous pouvez vérifier l'état d'isolement réseau de l'appareil à partir de la ligne de commande.

Un appareil isolé est automatiquement marqué par le tag **ISOLATED FROM NETWORK**. Une fois l'isolement du réseau désactivé, ce tag est automatiquement supprimée.

Pour obtenir des informations générales sur l'obtention d'une liste des appareils isolés par tag, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Limites de l'isolation réseau

Lorsque vous utilisez l'isolement du réseau, il est fortement recommandé de vous familiariser avec les restrictions.

Pour que l'isolation réseau fonctionne, l'application Kaspersky Endpoint Security doit être en cours d'exécution. Lors d'une panne de l'application Kaspersky Endpoint Security (lorsque l'application n'est pas en cours d'exécution), le blocage du trafic lorsque l'isolement du réseau est activée par les solutions Detection and Response n'est pas garanti.

DHCP et DNS ne sont pas automatiquement ajoutés aux exclusions de l'isolation réseau. Par conséquent, si l'adresse réseau d'une ressource a été modifiée pendant l'isolation réseau, l'application Kaspersky Endpoint Security ne pourra pas y accéder. Il en va de même pour les nœuds du serveur tolérant aux pannes KATA. Il n'est pas recommandé de modifier leurs adresses afin que Kaspersky Endpoint Security ne perde pas le contact avec eux.

Le serveur proxy n'est pas non plus automatiquement ajouté aux exclusions de l'isolation réseau, vous devez donc l'ajouter manuellement aux exclusions afin que l'application Kaspersky Endpoint Security ne perde pas la connexion avec le serveur qui assure l'intégration.

L'exclusion des processus de l'isolement du réseau par nom est prise en charge sur les appareils dotés d'un noyau version 4.18 ou ultérieure avec eBPF, la prise en charge de BTF et les fonctions tracepoints et kprobes activées pour le traçage du noyau.

Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode EDR Agent, nous recommandons ce qui suit lors de l'utilisation de l'isolement réseau :

- Utiliser le serveur proxy KSN pour interagir avec Kaspersky Security Network.
- Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation de l'application.

  S'il est impossible d'utiliser Kaspersky Security Center comme serveur proxy, il faut configurer les paramètres du serveur proxy requis et les ajouter aux exclusions.
- Spécifier Kaspersky Security Center comme source des mises à jour des bases de données.

Ces recommandations ne s'appliquent pas si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Activer ou désactiver manuellement l'isolation réseau d'un appareil dans Web Console

Vous pouvez activer l'isolement réseau d'un appareil à l'aide de Web Console uniquement lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Optimum.

Activer ou désactiver manuellement l'isolation réseau des appareils lorsqu'ils sont intégrés à la solution Kaspersky Endpoint Detection and Response Optimum

Pour activer ou désactiver manuellement l'isolement du réseau pour un appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Si nécessaire, sélectionnez un groupe d'administration, recherchez votre appareil et cliquez sur son nom.

3. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

4. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

5. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez **Agents intégrés** → **Endpoint Detection and Response**.

6. Dans la fenêtre qui s'ouvre, dans le groupe de paramètres **isolement du réseau**, effectuez l'une des opérations suivantes :

   - Cliquez sur le bouton **Isoler l'appareil du réseau** pour activer l'isolement réseau de l'appareil. Le bouton est disponible uniquement si le commutateur **Endpoint Detection and Response** est activé.

     Lorsque vous cliquez sur ce bouton, l'appareil est isolé pendant la période que vous avez définie dans les propriétés de la tâche *Activation de l'isolement réseau (NetworkIsolationStart)*.

   - Cliquez sur le bouton **Débloquer un appareil isolé** pour désactiver l'isolation réseau de l'appareil. Le bouton est disponible, que le commutateur **Endpoint Detection and Response** soit activé ou désactivé.

7. Cliquez sur le bouton **OK**.

Si vous avez activé l'isolement réseau de l'appareil, Kaspersky Endpoint Security attribuera le tag **ISOLATED FROM NETWORK** à l'appareil. Si vous avez désactivé l'isolation réseau d'un appareil, Kaspersky Endpoint Security supprimera ce tag de l'appareil.

Désactivation manuelle de l'isolement réseau d'un appareil lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou Kaspersky Endpoint Detection and Response (KATA)

Pour désactiver manuellement l'isolation réseau pour un appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil dont vous avez besoin dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response**.

7. Dans la section **Isolement réseau (EDR Expert (on-premises))**, cliquez sur le bouton **Débloquer un appareil isolé** pour désactiver l'isolement réseau de l'appareil.

Après avoir désactivé l'isolation réseau d'un appareil, Kaspersky Endpoint Security supprimera le tag **ISOLATED FROM NETWORK** de l'appareil.

Configuration de la durée d'isolement du réseau en mode automatique

Vous pouvez configurer des exclusions de l'isolement du réseau en mode automatique uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum.

L'isolement du réseau des appareils isolés à la suite de la tâche *Analyse IOC* est automatiquement désactivée après une période de temps spécifiée. Vous pouvez configurer cette période dans Web Console dans les propriétés de l'appareil et dans les propriétés de la stratégie. Les paramètres de l'isolement du réseau dans les propriétés de la stratégie de Web Console sont décrits dans l'annexe 5. Les paramètres de l'isolement du réseau dans les propriétés de l'appareil administré sont décrits dans le tableau ci-dessous.

Si un appareil est couvert par une stratégie, les paramètres spécifiés dans la stratégie sont appliqués ; le paramètre d'arrêt automatique de l'isolation réseau n'est pas disponible dans les propriétés de l'appareil. Si l'appareil n'est pas couvert par la stratégie, les paramètres spécifiés dans les propriétés de l'appareil sont appliqués.

Par défaut, l'application désactive l'isolation réseau 5 heures après son activation. Après avoir désactivé l'isolement du réseau, l'appareil peut fonctionner sur le réseau sans restrictions.

Configuration de la désactivation automatique de l'isolation réseau dans les propriétés de l'appareil

Pour configurer la désactivation automatique de l'isolement réseau de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response** et cliquez sur le lien **Endpoint Detection and Response Optimum**.

7. Dans le groupe de paramètres **Isolation réseau**, cliquez sur le lien **Configurer le déverrouillage de l'appareil**.

8. Dans la fenêtre ouverte **Configuration du déverrouillage de l'appareil**, cochez la case **Débloquer un appareil automatiquement isolé après** et dans le champ de saisie ci-dessous, indiquez la période en heures après laquelle l'appareil sera automatiquement déverrouillé.

9. Enregistrez vos modifications.

Configuration des paramètres de l'isolation réseau en mode manuel

Vous pouvez isoler manuellement un appareil du réseau uniquement lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum.

Si vous activez manuellement l'isolement du réseau pour un appareil, vous pouvez préconfigurer les paramètres d'isolement du réseau à l'aide de la tâche locale *Activation de l'isolement du réseau* (*NetworkIsolationStart*). Vous pouvez configurer des exclusions de l'isolation réseau et la durée de l'isolation réseau pour un appareil.

La tâche *Activation de l'isolation réseau* est préinstallée et ne s'exécute automatiquement que dans les cas suivants :

- Si vous avez cliqué sur le bouton **Isoler l'appareil du réseau** dans les propriétés de l'appareil.
- Si vous activez l'isolement réseau de l'appareil dans la fenêtre des détails de l'alerte.

Vous ne pouvez pas créer une nouvelle instance de la tâche *Activation de l'isolement du réseau* à l'aide du bouton **Ajouter** ou l'exécuter en cliquant sur le bouton **Exécuter**. La tâche est uniquement disponible dans les propriétés de l'appareil, où vous pouvez modifier ses paramètres avant d'activer l'isolement réseau de l'appareil.

Paramètres de la tâche *Activation de l'isolement du réseau* s'appliquent indépendamment du fait que l'appareil soit couvert ou non par la stratégie.

Pour configurer les paramètres de l'isolement réseau de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, accédez à l'onglet **Tâches**.

5. Dans la liste des tâches, cliquez sur la tâche *Activation de l'isolement du réseau*.

   La fenêtre des propriétés de la tâche s'ouvre.

6. Accédez à l'onglet **Paramètres de l'application**.

7. Cliquez sur le lien **Configurer les exclusions** pour ouvrir la fenêtre **Exclusions**.

8. Dans la fenêtre qui s'ouvre, utilisez les boutons au-dessus du tableau pour effectuer l'action souhaitée :

   - Si vous souhaitez ajouter des informations sur une connexion réseau exclue, faites-le de l'une des manières suivantes :

     - Cliquez sur le bouton **Ajouter** et saisissez les informations sur la connexion réseau.

     - Cliquez sur le bouton **Ajouter à partir d'un profil** et sélectionnez un profil réseau dans le dictionnaire.

   - Si vous souhaitez supprimer les informations sur une connexion réseau à exclure, cochez la case en regard de la connexion réseau à supprimer et cliquez sur le bouton **Supprimer**.

9. Cliquez sur le bouton **OK**.

10. Saisissez la durée requise d'isolement réseau de l'appareil en heures dans le champ **Isoler l'appareil pour**.

    La durée d'isolement du réseau par défaut est de 5 heures.

    La durée minimale d'isolement du réseau ne peut être inférieure à 1 heure.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Configuration des exclusions de l'isolement du réseau dans Web Console

Lorsque Kaspersky Endpoint Security est intégré à Endpoint Detection and Response Expert (on-premises), à Kaspersky Endpoint Detection and Response (KATA) ou à Kaspersky Managed Detection and Response, les exclusions de l'isolement du réseau sont configurées du côté de la solution Detection and Response. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises), l'aide de Kaspersky Anti Targeted Attack Platform ou l'aide de Kaspersky Managed Detection and Response.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez configurer les exclusions de l'isolement du réseau des manières suivantes :

- Dans les propriétés de la stratégie dans Web Console. Les exclusions configurées dans la stratégie sont appliquées lorsque l'isolement du réseau est automatiquement activé pour un appareil sous la stratégie.

- Dans les propriétés de l'appareil dans Web Console. Les exclusions configurées dans les propriétés de l'appareil sont appliquées lorsque l'isolement du réseau est automatiquement activé pour un appareil qui n'est pas couvert par la stratégie.

- Dans les paramètres de la tâche locale *Activation de l'isolement du réseau* (*NetworkIsolationStart*). Les exclusions configurées dans les propriétés de cette tâche sont appliquées lorsque vous activez manuellement l'isolement du réseau pour un appareil. Les paramètres de la tâche *Activation de l'isolement du réseau* s'appliquent, qu'une stratégie soit appliquée ou non à l'appareil.

Pour configurer les exclusions de l'isolement du réseau, l'application fournit une liste de *profils de réseau standard*. Les profils réseau sont constitués de règles qui garantissent le fonctionnement ininterrompu des appareils dotés des rôles du serveur DNS/DHCP et du client DNS/DHCP. Vous pouvez modifier les paramètres des profils de réseau standard et définir des exclusions manuellement.

L'ajout ou la suppression des exclusions de l'isolation réseau dans les propriétés de l'appareil n'est pas disponible si l'appareil est couvert par une stratégie.

Ajout d'une exclusion de l'isolation du réseau dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response**.
5. Dans le groupe **Isolement du réseau**, cliquez sur le lien **Exclusions**.
   Cette action ouvre une fenêtre contenant la liste des exclusions de l'isolation du réseau.
6. Vous pouvez exclure une connexion réseau des manières suivantes :
   - Cliquez sur **Ajouter** et saisissez les informations relatives à la connexion réseau.

     Vous pouvez ajouter une application pour laquelle le module ne bloquera pas les connexions réseau. Ce paramètre s'applique aux appareils avec une version de noyau à partir de 4.18 prenant en charge eBPF et BTF et avec les fonctions tracepoints et kprobes activées pour le traçage du noyau.
   - Cliquez sur le bouton **Ajouter à partir du profil** et sélectionnez un profil réseau dans le dictionnaire.
7. Enregistrez vos modifications.

Suppression d'une exclusion de l'isolation du réseau dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response**.
5. Dans le groupe **Isolement du réseau**, cliquez sur le lien **Exclusions**.
   Cette action ouvre une fenêtre contenant la liste des exclusions de l'isolation du réseau.
6. Cochez la case en regard de la connexion réseau et cliquez sur **Supprimer**.
7. Enregistrez vos modifications.

Mettre un fichier en quarantaine

Lors de la réaction aux menaces, Kaspersky Endpoint Detection and Response peut créer des tâches *Placer le fichier en Quarantaine*. Cette mesure est nécessaire pour minimiser les conséquences de la menace. La *Quarantaine* est un stockage local spécial sur l'ordinateur. L'utilisateur peut mettre en quarantaine les fichiers qu'il considère comme dangereux pour l'ordinateur. Les fichiers mis en quarantaine sont stockés chiffrés et ne menacent pas la sécurité de l'appareil.

Vous pouvez créer des tâches *Placer le fichier en Quarantaine* de la manière suivante :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Vous pouvez sélectionner le fichier à supprimer directement dans les détails de l'alerte. Kaspersky Endpoint Security lance alors l'assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

- À l'aide de l'Assistant de création d'une tâche.

  L'Assistant de création d'une tâche permet de saisir manuellement le chemin d'accès au fichier ou au répertoire, ainsi que le hachage du fichier à supprimer. Vous pouvez également gérer des paramètres supplémentaires de la tâche, comme la configuration de la planification de la tâche.

- Dans les paramètres de la tâche *Analyse IOC*.

  Si la tâche *Analyse IOC* détecte un fichier qui peut compromettre les données, vous pouvez mettre ce fichier en quarantaine directement à partir des résultats de l'analyse IOC (**Paramètres de l'application → Résultats de l'analyse IOC**). Kaspersky Endpoint Security lance alors l'assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

La taille du fichier ne doit pas dépasser 100 Mo.

Comment créer une tâche Placer le fichier en Quarantaine

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Placer le fichier en Quarantaine**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la nouvelle tâche.

7. La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Dans la liste des fichiers, cliquez sur **Ajouter**.

   L'Assistant d'ajout de fichiers démarre.

10. Pour ajouter un fichier, vous devez saisir le chemin d'accès au fichier ou le chemin d'accès au répertoire, ainsi que le hachage du fichier.

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security déplace alors des fichiers dans la Quarantaine.

Si le fichier est verrouillé par un autre processus, la tâche s'affiche comme *Terminée*, mais le fichier lui-même n'est mis en quarantaine qu'après le redémarrage de l'ordinateur. Après avoir redémarré l'ordinateur, confirmez que le fichier est supprimé.

La tâche *Placer le fichier en Quarantaine* peut se terminer par l'erreur *Accès interdit* si vous essayez de mettre en quarantaine un fichier exécutable en cours d'exécution. Créez une tâche Terminer le processus pour le fichier et réessayez.

La tâche *Placer le fichier en Quarantaine* peut se terminer par l'erreur *Espace insuffisant dans le Stockage en ligne* si vous essayez de mettre en quarantaine un fichier trop volumineux. Effacez la quarantaine ou augmentez la taille de la quarantaine. Puis réessayez.

Reception d'un fichier depuis un appareil

Vous pouvez obtenir des fichiers à partir des ordinateurs des utilisateurs. Par exemple, vous pouvez configurer pour recevoir un fichier journal des événements généré par un logiciel tiers. À la suite de l'exécution de la tâche, une copie du fichier est enregistrée dans la Quarantaine. La *Quarantaine* est un stockage local spécial sur l'ordinateur. Vous pouvez télécharger ce fichier depuis la Quarantaine vers votre ordinateur à l'aide de Web Console (**Opérations → Stockages → Quarantaine**). Le fichier d'origine sur l'appareil de l'utilisateur reste dans le répertoire d'origine.

Dans Kaspersky Security Center, dans la liste des fichiers mis en quarantaine, tous les fichiers reçus via la tâche *Obtenir le fichier* auront l'état *Infecté*, quels que soient les résultats de l'analyse des fichiers.

La taille du fichier ne doit pas dépasser 100 Mo.

Comment créer une tâche Obtenir le fichier

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Obtenir le fichier**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la nouvelle tâche.

7. La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Dans la liste des fichiers, cliquez sur **Ajouter**.

   L'Assistant d'ajout de fichiers démarre.

10. Pour ajouter un fichier, vous devez saisir le chemin d'accès au fichier ou le chemin d'accès au répertoire, ainsi que le hachage du fichier.

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security crée une copie du fichier et la place dans la Quarantaine. Vous pouvez télécharger le fichier de la Quarantaine dans Web Console.

La tâche *Obtenir le fichier* se termine avec une erreur si :

- le fichier spécifié n'a pas été trouvé ;
- les données du fichier sont incorrectes (nom de fichier ou somme de contrôle) ;
- les privilèges sont insuffisants pour effectuer des actions sur le fichier spécifié ;
- le fichier spécifié est bloqué ;

- il n'y pas assez d'espace dans la quarantaine ;
- le fichier spécifié est trop volumineux (plus de 100 Mo).

Suppression d'un fichier de votre appareil

Vous pouvez supprimer des fichiers à distance à l'aide de la tâche *Supprimer le fichier*. Par exemple, vous pouvez supprimer à distance un fichier lorsque vous répondez à des menaces.

Comment créer une tâche Supprimer le fichier

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.
2. Cliquez sur **Ajouter**.
   L'Assistant de création de tâche démarre.
3. Configurez les paramètres de la tâche :
   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux**.
   b. Dans la liste déroulante **Type de tâche**, choisissez **Supprimer le fichier**.
   c. Dans le champ **Nom de la tâche**, saisissez une courte description.
   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.
4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur **Suivant**.
5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.
   La nouvelle tâche apparaît dans la liste des tâches.
6. Cliquez sur la nouvelle tâche.
7. La fenêtre des propriétés de la tâche s'ouvre.
8. Sélectionnez l'onglet **Paramètres de l'application**.
9. Pour ajouter un fichier, vous devez saisir le chemin d'accès au répertoire et le hachage du fichier.
10. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.
11. Programmez l'exécution de la tâche.
12. Enregistrez vos modifications.
13. Cochez la case en regard de la tâche.
14. Cliquez sur **Démarrer**.

Kaspersky Endpoint Security supprime alors le fichier de l'ordinateur. Si le fichier est verrouillé par un autre processus, la tâche s'affiche comme *Progression*, mais le fichier lui-même n'est supprimé qu'après le redémarrage de l'ordinateur. Après avoir redémarré l'ordinateur, confirmez que le fichier est supprimé.

Démarrage du processus

Vous pouvez lancer des fichiers à distance à l'aide de la tâche *Démarrage du processus*. Par exemple, vous pouvez exécuter à distance un utilitaire qui crée le fichier de configuration de l'ordinateur. Ensuite, vous pouvez utiliser la tâche *Obtenir le fichier* pour recevoir le fichier créé dans Kaspersky Security Center Web Console.

Si SELinux est en mode `Enforcing` dans votre système d'exploitation, pour lancer la tâche *Démarrage du processus*, vous devez effectuer une configuration supplémentaire de SELinux.

Comment configurer SELinux pour exécuter la tâche « Lancer le processus »

Si vous prévoyez d'utiliser SELinux en mode `Enforcing` sur votre système d'exploitation, vous devez gérer en outre les paramètres SELinux afin d'exécuter les actions de réponse lors de l'intégration avec les solutions Detection and Response.

Cette configuration SELinux requiert les privilèges root.

Pour configurer SELinux pour les actions de réponse :

1. Placez le système SELinux en mode non bloquant :

   - Si SELinux est activé, exécutez la commande suivante :

     ```
     Placez le système SELinux en mode non bloquant

     setenforce Permissive
     ```

   - Si SELinux est désactivé, définissez `SELINUX=permissive` dans le fichier de configuration /etc/selinux/config, puis redémarrez le système d'exploitation.

2. Assurez que l'utilitaire semanage est installé dans le système. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.

3. Exécutez toutes les tâches permettant d'effectuer les actions de réponse que vous souhaitez utiliser dans le cadre de l'intégration aux solutions Detection and Response.

4. Assurez-vous que le fichier audit.log ne contient aucune erreur.

   ```
   Afficher le fichier audit.log

   grep kesl /var/log/audit/audit.log
   ```

5. Si des erreurs sont présentes dans le fichier audit.log, créez et chargez un nouveau module de règles basé sur les enregistrements de blocage pour corriger les erreurs, puis exécutez à nouveau les tâches d'actions de réponse.

   ```
   Créez et chargez un nouveau module de règles sur la base des enregistrements de blocage :

   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

6. Placez le système SELinux en mode bloquant.

```
setenforce Enforcing
```

Comment créer une tâche Démarrage du processus

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Démarrage du processus**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la nouvelle tâche.

7. La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Saisissez la commande de démarrage du processus :

   - **Commande exécutable**. Champ de saisie de la commande de démarrage du processus.

     Par exemple, si vous souhaitez exécuter l'utilitaire `klnagchk`, qui vérifie la connexion au Serveur d'administration, `/opt/kaspersky/klnagent/bin/klnagchk`.

   - **Arguments de ligne de commande (facultatif)**. Un champ de saisie des arguments de la ligne de commande permettant de transmettre des informations supplémentaires au script, à l'utilitaire ou à l'application lors de son lancement.

     Par exemple, vous pouvez saisir l'argument `-logfile /tmp/klnagchk.log`. Cet argument indique à l'outil d'enregistrer le résultat dans un fichier nommé `klnagchk.log` dans `/tmp`. Si vous devez transmettre plusieurs arguments, vous devez les séparer par des espaces.

   - **Chemin d'accès au dossier de travail (facultatif)**. Champ de saisie du chemin d'accès au répertoire de travail dans lequel le processus place les fichiers.

     Par exemple, vous pouvez saisir `/tmp` et exécuter l'utilitaire `klnagchk` avec les arguments suivants : `-logfile klnagchk.log -savecert certificate.cer`. Dans ce cas, les deux fichiers sont créés dans `tmp`.

10. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

11. Programmez l'exécution de la tâche.

12. Enregistrez vos modifications.

13. Cochez la case en regard de la tâche.

14. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security exécute alors la commande en mode silencieux et lance le processus. Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats d'exécution**.

Terminer le processus

Vous pouvez mettre fin aux processus à distance à l'aide de la tâche *Fin du processus*. Par exemple, vous pouvez mettre fin à distance à un processus lancé à la suite d'une activité malveillante.

Si vous souhaitez interdire l'exécution d'un fichier, vous pouvez configurer le module Prévention de l'exécution. Vous pouvez interdire l'exécution de fichiers exécutables, de scripts et de fichiers au format Office.

Création d'une tâche Fin du processus

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Linux**.

   b. Dans la liste déroulante **Type de tâche**, choisissez *Fin du processus*.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la nouvelle tâche.

7. La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Pour mettre fin au processus, vous devez sélectionner le fichier du processus auquel vous souhaitez mettre fin. Vous pouvez sélectionner un fichier d'une des manières suivantes :

   - Saisissez le nom complet du fichier.
   - Saisissez le hachage du fichier et le chemin d'accès au fichier.
   - Saisissez le PID du processus (uniquement pour les tâches locales).
   - Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

10. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.
11. Programmez l'exécution de la tâche.
12. Enregistrez vos modifications.
13. Cochez la case en regard de la tâche.
14. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security arrête alors ce processus sur l'ordinateur. Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats**.

Prévention de l'exécution des objets

Vous pouvez appliquer cette action de réponse lors de l'intégration avec les solutions Kaspersky Detection and Response, à partir desquelles Kaspersky Endpoint Security reçoit des règles de prévention de l'exécution.

Si un objet correspond à une règle, Kaspersky Endpoint Security empêche l'exécution de cet objet.

Prévention de l'exécution des objets EDR Expert (on-premises)

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Detection and Response Expert (cloud) ou Kaspersky Endpoint Detection and Response (KATA), vous pouvez configurer des règles de blocage de l'exécution des objets dans la console de la solution correspondante.

Si l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises) ou le module Kaspersky Endpoint Detection and Response (KATA) est activée, vous pouvez activer ou désactiver la prévention de l'exécution des objets dans les propriétés de la stratégie (**Paramètres de l'application → Configuration des agents intégrés → Endpoint Detection and Response Expert (on-premises)**).

Pour activer la prévention de l'exécution des objets, placez le commutateur sur **Prévention de l'exécution ACTIVÉE**.

Prévention du lancement des objets (EDR Optimum)

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez configurer la Prévention de l'exécution des objets et les règles de prévention de l'exécution dans Web Console.

Activation de la prévention de l'exécution des objets dans une stratégie de Kaspersky Security Center

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response**.
5. Rendez-vous dans l'onglet **Prévention de l'exécution**.
6. Réglez le commutateur sur **Prévention de l'exécution ACTIVÉE**.
7. Sélectionnez une action lors du démarrage ou de l'ouverture d'un objet

   - **Bloquer et ajouter au journal des événements**. L'application bloque l'exécution des objets ou l'ouverture de documents qui satisfont aux critères des règles de prévention, et consigne dans le journal des événements un événement relatif aux tentatives d'exécution d'objets ou d'ouverture de documents.
   - **Ajouter au journal des événements**. L'application consigne dans le journal des événements un événement relatif aux tentatives d'exécution d'objets exécutables ou d'ouverture de documents qui satisfont aux critères des règles de prévention, mais ne bloque pas réellement leur exécution ou leur ouverture.
8. Enregistrez vos modifications.

Activation de la Prévention de l'exécution des objets dans les propriétés de l'appareil administré

1. Dans Web Console, accédez à **Gestion des ressources → Actifs (Appareils)**.
2. Cliquez sur le lien contenant le nom de l'appareil souhaité.
3. La fenêtre des propriétés de l'appareil sélectionné s'ouvre ; dans cette fenêtre, accédez à l'onglet **Applications** et cliquez sur le lien <nom de l'application **Kaspersky Endpoint Security**>.

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.
   4. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response**.
   5. Rendez-vous dans l'onglet **Prévention de l'exécution**.
   6. Réglez le commutateur sur **Prévention de l'exécution ACTIVÉE**.

7. Sélectionnez une action lors du démarrage ou de l'ouverture d'un objet

   - **Bloquer et ajouter au journal des événements**. L'application bloque l'exécution des objets ou l'ouverture de documents qui satisfont aux critères des règles de prévention, et consigne dans le journal des événements un événement relatif aux tentatives d'exécution d'objets ou d'ouverture de documents.

   - **Ajouter au journal des événements**. L'application consigne dans le journal des événements un événement relatif aux tentatives d'exécution d'objets exécutables ou d'ouverture de documents qui satisfont aux critères des règles de prévention, mais ne bloque pas réellement leur exécution ou leur ouverture.

8. Enregistrez vos modifications.

4. Sélectionnez l'onglet **Paramètres de l'application**.

5. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response**.

6. Accédez à la sous-section **Prévention de l'exécution**.

7. Réglez le commutateur sur **Prévention de l'exécution ACTIVÉE**.

8. Sélectionnez le mode de prévention de l'exécution des objets :

   - **Bloquer**. Dans ce mode, l'application bloque le lancement des objets ou l'ouverture de documents répondant aux critères des règles de refus, et enregistre dans le journal des événements un événement concernant les tentatives de lancement des objets ou d'ouverture de documents.

   - **Informer**. Dans ce mode, l'application enregistre dans le journal des événements un événement relatif aux tentatives de lancement des objets exécutables ou d'ouverture de documents répondant aux critères des règles de refus, mais ne bloque pas leur lancement ou leur ouverture. Ce mode est sélectionné par défaut.

9. Enregistrez vos modifications.

L'activation et la désactivation de la prévention du lancement des objets dans les propriétés de l'appareil ne sont pas disponibles si l'appareil est couvert par une stratégie.

Ajout d'une règle de Prévention de l'exécution des objets du module EDR Optimum dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Le cas échéant, cochez la case **Utiliser un emplacement sensible à la casse**.

5. Dans les propriétés de la stratégie ou de l'appareil administré, cliquez sur le bouton **Ajouter** dans la barre d'outils située au-dessus de la liste des règles de prévention de l'exécution des objets.

6. Dans la fenêtre qui s'ouvre, saisissez le nom de prévention de lancement.

7. Spécifiez l'état de la règle de prévention de l'exécution en plaçant le commutateur sur la position appropriée.

8. Dans la liste déroulante **Type**, sélectionnez le type d'objet que vous souhaitez bloquer :

   - **Fichier exécutable**.
   - **Script**.
   - **Fichier de l'application Office**.

   Si vous sélectionnez le mauvais type d'objet, l'application ne bloquera pas le fichier ou le script.

9. Pour ajouter un objet, indiquez le chemin d'accès à l'objet et/ou la somme de contrôle de l'objet (hachage SHA256 ou MD5 du fichier) dans le champ correspondant.

10. Enregistrez vos modifications.

    La règle créée est ajoutée à la liste des règles dans le groupe de paramètres **Prévention du lancement des objets**.

Kaspersky Endpoint Security contrôle l'exécution des fichiers exécutables et des scripts, ainsi que l'ouverture des fichiers d'applications bureautiques sur l'appareil. La prevention de lancement des objets prend en charge un ensemble spécifique d'extensions des fichiers des applications Office et un ensemble spécifique d'interpréteurs de script. Suite à la prévention du lancement des objets, la propagation de la menace peut être stoppée.

La fonctionnalité de prévention du lancement des objets est disponible dans l'application Kaspersky Endpoint Security si l'une des conditions suivantes est remplie :

- L'intégration à la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premises) est activé.
- L'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) est activée, et le module EDR Expert (cloud) est activé.

Si le mode de blocage de l'interception des opérations sur les fichiers n'est pas activé, la prévention de l'exécution des objets fonctionne en mode de notification, quel que soit le mode de fonctionnement défini.

Par défaut, la prévention du lancement des objets est désactivée. L'activation de la prévention du lancement des objets peut affecter la vitesse de lancement des applications dans le système d'exploitation.

Pour que la prévention du lancement des objets fonctionne, vous devez activer l'application des règles de prévention du lancement des objets.

Limitations et particularités de la prévention de l'exécution des objets

Limites de prévention du lancement des objets

Les restrictions suivantes existent pour empêcher le lancement des objets :

- Kaspersky Endpoint Security ne bloque pas les objets spécifiés dans les règles de prévention du lancement avant le lancement de l'application.
- Kaspersky Endpoint Security ne bloque pas les fichiers ouverts avant la création ou la modification de la règle de prévention du lancement.
- L'application Kaspersky Endpoint Security ne bloque pas le travail avec les objets qui ont été lancés avant la création ou la modification de la règle de prévention du lancement et qui relèvent des règles nouvellement définies.
- Certains fichiers peuvent être critiques pour le fonctionnement du système d'exploitation et de l'application. Prévention de lancement de tels fichiers peut perturber le fonctionnement du système.

Il n'est pas recommandé de créer plus de 50000 règles de démarrage car cela pourrait entraîner une instabilité du système.

Particularités de la prévention de l'exécution des objets lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response (KATA)

Lorsque l'application Kaspersky Endpoint Security est intégrée à Kaspersky Endpoint Detection and Response Expert (on-premises) ou à Kaspersky Endpoint Detection and Response (KATA), elle utilise les *règles de prévention de l'exécution des objets du module EDR Expert (on-premises)*. L'application reçoit ces règles de Kaspersky Endpoint Detection and Response Expert (on-premises) ou de Kaspersky Endpoint Detection and Response (KATA).

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou Kaspersky Endpoint Detection and Response (KATA), vous pouvez :

- Activer ou désactiver l'application des règles de prévention de l'exécution des objets du module EDR Expert (on-premises) dans Web Console ou dans la Console d'administration.

  Lorsque des règles de prévention de l'exécution sont déclenchées, Kaspersky Endpoint Security envoie un rapport à Endpoint Detection and Response Expert (on-premises) ou à Kaspersky Anti Targeted Attack Platform. Pour plus de détails, consultez l'aide de la solution correspondante.
- Afficher la liste des règles de prévention de l'exécution des objets du module EDR Expert (on-premises) via la ligne de commande.

Particularités de la Prévention de l'exécution des objets lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response (KATA), l'application utilise les *règles de la prévention du lancement des objets du module EDR Optimum*. Vous créez ces règles manuellement dans Web Console. Vous pouvez également créer automatiquement des règles de prévention de l'exécution dans la fenêtre des détails de l'alerte.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez :

- Activer ou désactiver l'application des règles de prévention de l'exécution des objets du module EDR Optimum dans Web Console.
- Créer et configurer des règles de prévention de l'exécution des objets du module EDR Optimum dans Web Console.

Vous pouvez également créer automatiquement une règle de prévention de l'exécution pour un objet en empêchant l'exécution d'un fichier dans la fenêtre des détails de l'alerte. La règle de la prévention du lancement sera ajoutée à la stratégie du groupe d'administration auquel appartient l'appareil.

Vous pouvez bloquer l'exécution des fichiers dans la fenêtre des détails de l'alerte uniquement si l'appareil est couvert par une stratégie.

- Afficher dans ligne de commande la liste des règles de la prévention du lancement des objets du module DR Optimum.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, la prévention du lancement des objets peut fonctionner selon l'un des deux modes suivants :

- **Bloquer**. Dans ce mode, l'application bloque le lancement des objets ou l'ouverture de documents répondant aux critères des règles de refus, et enregistre un événement dans le journal concernant les tentatives de lancement des objets ou d'ouverture de documents.

  L'application Kaspersky Endpoint Security bloque l'exécution d'un script interdit par la règle de prévention du lancement, même s'il est importé par un script autorisé.

- **Informer**. Dans ce mode, l'application enregistre dans le journal un événement relatif aux tentatives de lancement des objets exécutables ou d'ouverture de documents répondant aux critères des règles de refus, mais ne bloque pas leur lancement ou leur ouverture. Ce mode est sélectionné par défaut.

Travailler avec la quarantaine

La *quarantaine* est un stockage spécial sur l'appareil où sont placés les fichiers qui peuvent être infectés par des virus ou qui sont incurables au moment de la détection. La quarantaine vous permet d'isoler un fichier pour une analyse plus approfondie. Les fichiers mis en quarantaine sont stockés chiffrés et ne menacent pas la sécurité de l'appareil. Contrairement à la quarantaine, la sauvegarde est conçu pour stocker des copies de sauvegarde des fichiers dans lesquels un code malveillant a été détecté et qui ont été supprimés ou modifiés au cours du processus de traitement.

L'application utilise la quarantaine uniquement lorsqu'elle est intégrée avec les solutions Detection and Response pour effectuer les actions de réponse aux menaces recommandées. Lors de l'intégration de l'application avec Kaspersky Endpoint Detection and Response Optimum ou avec Kaspersky Managed Detection and Response, vous pouvez également mettre manuellement en quarantaine les fichiers que vous considérez comme dangereux pour votre appareil.

Par défaut, le répertoire /var/opt/kaspersky/kesl/common/objects-backup/ est utilisé pour stocker les fichiers mis en quarantaine. Ce répertoire stocke également les objets de la sauvegarde. Vous pouvez modifier le répertoire dans lequel les objets de sauvegarde et de quarantaine sont stockés à l'aide de la ligne de commande.

Les fichiers en quarantaine peuvent contenir des données personnelles. L'accès root est requis pour accéder aux fichiers mis en quarantaine.

Vous pouvez configurer les paramètres de la Quarantaine sur un appareil à l'aide d'une stratégie dans Web Console ou dans la Console d'administration, ou à l'aide de la ligne de commande. Vous pouvez configurer les paramètres suivants de la quarantaine :

- Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Par défaut, un événement est généré lorsque la quarantaine est pleine à 90 %.
- Volume maximal de la quarantaine en mégaoctets. Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime automatiquement les fichiers les plus anciens de la quarantaine. Par défaut, la taille maximale de la quarantaine est de 200 Mo si l'application est utilisée en mode standard ou en mode EDR Agent, et de 100 Mo si l'application est utilisée en mode Light Agent.
- Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine (ce paramètre est configurable uniquement à l'aide de la ligne de commande).

Comment gérer les paramètres de la Quarantaine dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Rapports et stockage**.
5. Dans la section **Quarantaine**, configurez les paramètres suivants :
   - **Limiter la taille de la Quarantaine**. Limitation de la taille de la Quarantaine à la valeur indiquée en mégaoctets. La case est cochée par défaut.
   - **Taille maximale de la Quarantaine (Mo)**. Si le paramètre **Limiter la taille de la Quarantaine** est activé, vous pouvez indiquer la taille maximale de la Quarantaine en mégaoctets (200 Mo par défaut). La taille de la Quarantaine ne doit pas dépasser 999 999 Mo.
   - **Notifier lorsque la quarantaine est pleine**. Notifications lorsque la Quarantaine atteint ce pourcentage de remplissage. La case est cochée par défaut.

     Vous pouvez indiquer le pourcentage à partir duquel une notification est envoyée (90 % par défaut).
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Mise en quarantaine des fichiers

Certains fichiers peuvent être critiques pour le fonctionnement du système d'exploitation et de l'application. La mise en quarantaine de ces fichiers peut perturber le fonctionnement du système.

La mise en quarantaine d'un fichier n'est possible que si l'une des conditions suivantes est remplie :

- L'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premises) est activé.
- L'intégration de Kaspersky Endpoint Security avec Kaspersky Managed Detection and Response est activée et le module MDR est activé.

Le répertoire pour stocker les objets de quarantaine doit être accessible en écriture.

En cas d'intégration avec Kaspersky Endpoint Detection and Response (on-premises) ou Kaspersky Endpoint Detection and Response (KATA), les fichiers peuvent être mis en quarantaine de l'une des manières suivantes :

- Suite à l'exécution d'une tâche configurée du côté de la solution Detection and Response correspondante. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises) ou l'aide de Kaspersky Anti Targeted Attack Platform.
- À la suite de l'exécution de la tâche d'analyse IOC sur la mémoire du processus.

Lorsqu'ils sont intégrés à Kaspersky Managed Detection and Response, les fichiers sont mis en quarantaine de l'une des manières suivantes :

- Suite à l'exécution d'une tâche configurée du côté de Kaspersky Managed Detection and Response.
- Suite à l'exécution de la commande de gestion de la quarantaine sur l'appareil.

Pour plus d'informations sur l'utilisation de la quarantaine lors de l'intégration avec Kaspersky Managed Detection and Response, consultez l'aide de Kaspersky Managed Detection and Response.

Lorsqu'ils sont intégrés à Kaspersky Endpoint Detection and Response Optimum, les fichiers sont mis en quarantaine de l'une des manières suivantes :

- Automatiquement suite à la détection d'indicateurs de compromission.
- Suite à l'exécution de la tâche *Mettre en quarantaine un fichier*, que vous pouvez créer dans Web Console.
- Suite à l'exécution de la commande de gestion de la quarantaine sur l'appareil.
- Suite à l'exécution de la recommandation indiquée dans les détails de l'alerte.

Pour plus d'informations sur l'utilisation de la quarantaine lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Travailler avec des fichiers en quarantaine

Vous pouvez travailler avec des fichiers en quarantaine :

- Dans Kaspersky Security Center, dans la liste générale des fichiers mis en quarantaine par les applications Kaspersky.

  Pour effectuer des actions sur les fichiers en quarantaine dans Kaspersky Security Center, vous devez activer le transfert de données sur les fichiers en quarantaine vers le Serveur d'administration.

- Localement sur l'appareil à l'aide de la ligne de commande.

Vous pouvez afficher des informations sur les fichiers en quarantaine, supprimer et restaurer les fichiers depuis la quarantaine.

La restauration, la suppression et la récupération d'un fichier de quarantaine sont disponibles, que l'intégration avec les solutions Detection and Response soit activée ou non, et que l'appareil soit couvert par une stratégie ou non.

Une liste générale des fichiers mis en quarantaine par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans la Console d'administration (**Avancés** → **Stockages** → **Quarantaine**) et dans Web Console (**Opérations** → **Stockages** → **Quarantaine**). Kaspersky Security Center ne copie pas les fichiers depuis les stockages de la quarantaine vers le Serveur d'administration ; tous les fichiers sont placés dans les stockages de la quarantaine sur les appareils clients. Pour obtenir des informations détaillées sur la gestion des fichiers en quarantaine dans Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Le fichier mis en quarantaine est restauré à son emplacement d'origine selon les paramètres spécifiés. L'étiquette de mandat (uniquement sur les appareils exécutant Astra Linux) et les attributs (y compris immutable et append-only) du fichier source sont conservés lors de la restauration. Un fichier doté des attributs immutable et append-only ne peut être restauré uniquement qu'à un emplacement spécifié où le fichier original n'existe pas, ou à l'emplacement original mais avec un autre nom. La restauration d'un fichier mis en quarantaine vers un autre répertoire ou vers son emplacement d'origine sous un nom différent nécessite les privilèges root.

Une fois la récupération terminée, l'application supprime la copie du fichier récupéré de la quarantaine.

La restauration d'un fichier depuis la quarantaine échoue avec une erreur dans les cas suivants :

- Le fichier à restaurer est introuvable dans le stockage de la quarantaine.
- Le nom du fichier en cours de restauration est mal orthographié ou dans une casse incorrecte.
- L'identifiant du fichier est incorrect.
- Le répertoire de destination a été supprimé, déplacé, renommé ou vous n'êtes pas autorisé à y accéder.

  Dans ce cas, l'application déplace le fichier vers le répertoire /var/opt/kaspersky/kesl/common/restored/. Vous pouvez déplacer manuellement le fichier de ce répertoire vers le répertoire souhaité.
- Un fichier du même nom existe déjà au chemin spécifié.
- Il n'y a pas assez d'espace sur l'appareil.

- Sur les appareils exécutant Astra Linux uniquement : l'étiquette de capacité du fichier est supérieure à celle du répertoire de destination.
- Uniquement sur les appareils exécutant le système d'exploitation Astra Linux : le niveau de capacité du fichier est inférieur à celui du répertoire de destination, et l'indicateur ccnr n'est pas défini pour ce répertoire.

La suppression d'un fichier depuis la quarantaine échoue avec une erreur dans les cas suivants :

- Le fichier à supprimer est introuvable dans le stockage de la quarantaine.
- Le nom du fichier à supprimer est mal orthographié ou dans une casse incorrecte.
- L'identifiant du fichier est incorrect.

Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum est une solution conçue pour protéger l'infrastructure informatique d'une organisation contre les menaces telles que les exploits, les ransomwares, les attaques sans fichier et l'utilisation de fichiers système légitimes par des outils malveillants pour endommager les appareils ou les données.

L'application Kaspersky Endpoint Security 12.5 for Linux est compatible avec Kaspersky Endpoint Detection and Response Optimum version 3.1.

L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (ci-après, *EDR Optimum*).

Pour l'administration centralisée de l'application Kaspersky Endpoint Security avec le module EDR Optimum, utilisez Kaspersky Security Center Windows 15.1 ou Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Fonctionnement de Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum surveille et analyse l'évolution des menaces, et fournit des informations sur une attaque potentielle au responsable de la sécurité ou à l'administrateur, ce qui les aide à exécuter des actions de réponse aux menaces en temps opportun.

Kaspersky Endpoint Detection and Response Optimum utilise les outils d'analyse des menaces suivants (Threat Intelligence) :

- L'infrastructure de services cloud Kaspersky Security Network (ci-après également KSN), donnant accès à la base de connaissances opérationnelles de Kaspersky sur la réputation des fichiers, des sites et des logiciels.
- Intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations sur la réputation des fichiers et des sites.
- Base de données des menaces de Kaspersky Threats.

En interagissant avec Kaspersky Endpoint Detection and Response Optimum, l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

- Envoyer les données d'événements sur les appareils vers Kaspersky Security Center. Kaspersky Endpoint Security envoie à Kaspersky Security Center des données de surveillance sur les processus, les connexions réseau ouvertes et les fichiers modifiés, ainsi que des données sur les menaces détectées par l'application et des données sur les résultats du traitement de ces menaces.
- Effectuer les actions de réponse visant à garantir les fonctions de sécurité sur la base des commandes reçues de Kaspersky Security Center.

Configuration de l'intégration de Kaspersky Endpoint Detection and Response Optimum

Conditions préalables

Avant de configurer l'intégration de Kaspersky Endpoint Detection and Response Optimum :

- Ajoutez la clé de licence EDR Optimum à l'application si vous avez acheté une licence distincte pour utiliser cette fonctionnalité.

  Si vous utilisez Kaspersky Endpoint Security sous une licence qui inclut Kaspersky Endpoint Detection and Response Optimum, aucune action n'est requise.

  > Si Kaspersky Endpoint Security est utilisé en mode Light Agent, la clé de licence est ajoutée à la SVM.

- Assurez-vous que les éléments suivants sont activés et fonctionnent :
  - Kaspersky Security Network en mode standard ou étendu :

    > Pour un fonctionnement plus efficace de Kaspersky Endpoint Detection and Response Optimum, il est recommandé d'utiliser Kaspersky Security Network en mode avancé.

  - Les modules suivants de l'application Kaspersky Endpoint Security :
    - Protection contre les fichiers malicieux.
    - Détection comportementale.

  Pour garantir l'exhaustivité de la télémétrie et créer une chaîne de développement de la menace dans Kaspersky Security Center, vous devez également activer Protection contre les menaces Internet.

Vous pouvez également activer la prévention du lancement des objets.

Étapes essentielles de la configuration

1. **Installer le plug-in d'administration de Kaspersky Endpoint Detection and Response Optimum**

   Le plug-in d'administration de Kaspersky Endpoint Detection and Response Optimum est un plug-in unique permettant de travailler avec des agents sous Windows, Mac et Linux et est requis pour afficher et visualiser les détails des alertes. Pour obtenir une description de la procédure d'installation, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

   Si votre infrastructure utilise Kaspersky Security Center Cloud Console pour administrer Kaspersky Endpoint Detection and Response Optimum, le plug-in est installé par défaut.

2. **Configurer les paramètres d'intégration de Kaspersky Endpoint Detection and Response Optimum**

   Vous pouvez la configurer :

   - À l'aide de la Web Console (console Kaspersky Security Center et/ou Console OSMP).
   - À l'aide de la ligne de commande.

   > La gestion du module EDR Optimum à l'aide de la Console d'administration de Kaspersky Security Center n'est pas prise en charge.

3. **Activer le transfert de données vers le Serveur d'administration**

   Pour que toutes les fonctionnalités de Kaspersky Endpoint Detection and Response Optimum fonctionnent, vous devez configurer les paramètres suivants :

   - Activez l'envoi des informations sur les fichiers dans la sauvegarde et dans la quarantaine vers le stockage de Kaspersky Security Center. Pour ce faire, vous devez cocher les cases dans les propriétés de la stratégie :
     - **À propos des fichiers de la sauvegarde**.
     - **À propos des fichiers de quarantaine**.
   - Autoriser l'affichage de la liste d'alertes Pour ce faire, vous devez activer le commutateur **Afficher les alertes EDR** dans la fenêtre principale de Web Console dans la section **Paramètres → Paramètres de l'interface**.

     > Paramètre **Afficher les alertes EDR** non disponible dans les versions de Web Console inférieures à 15.1. Vous pouvez accéder aux alertes EDR depuis le Rapport sur les menaces dans la console de Kaspersky Security Center.

   - Activez la transmission des informations sur les événements des applications tierces sur les appareils administrés. Pour ce faire, exécutez la commande suivante sur l'appareil administré :

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > L'activation de ce paramètre peut augmenter considérablement la charge du système d'exploitation.

4. **Vérifier que la connexion à Kaspersky Endpoint Detection and Response Optimum a été établie correctement**

   Vérifiez l'état de Kaspersky Endpoint Detection and Response Optimum de la manière qui vous convient.

L'intégration de Kaspersky Endpoint Detection and Response Optimum est configurée. Lorsqu'une menace est détectée, une alerte est générée. Dans la fenêtre des détails de l'alerte, vous pouvez consulter les informations sur la menace et effectuer des actions de réponse.

Comment activer l'intégration EDR Optimum

Dans Web Console, vous pouvez activer ou désactiver le module EDR Optimum et configurer l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans les propriétés de la stratégie.

Comment activer l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Activez le commutateur **Endpoint Detection and Response ACTIVÉ**.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans la ligne de commande

Pour activer le module EDR Optimum, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Gestion des actifs** → **Actifs (appareils)**.
2. Cliquez sur le lien contenant le nom de l'appareil souhaité.
3. La fenêtre des propriétés de l'appareil sélectionné s'ouvre ; dans cette fenêtre, accédez à l'onglet **Applications** et cliquez sur le lien <Kaspersky Endpoint Security application name>.
4. Accédez à l'onglet **Paramètres de l'application**, cliquez sur la section **Detection and Response**, puis cliquez sur le lien **Endpoint Detection and Response Optimum**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, définissez le commutateur sur **Endpoint Detection and Response Optimum activé** pour activer l'intégration.
6. Si nécessaire, gérez les paramètres suivants :

   - Durée du blocage de l'appareil dans le cadre de l'isolement automatique du réseau.

     Cliquez sur le lien **Configurer le déblocage de l'appareil** et indiquez la durée de blocage.
   - Exclusions de l'isolement automatique du réseau
7. Enregistrez vos modifications.

L'appareil administré est configuré pour l'intégration avec Kaspersky Endpoint Detection and Response Optimum.

Comment vérifier que l'intégration d'EDR Optimum est opérationnelle

Consultez les informations sur les états d'intégration possibles et les cas dans lesquels ils peuvent être affichés.

Vous pouvez tester le module EDR Optimum de l'une des manières suivantes :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

  L'intégration EDR Optimum s'affiche avec l'état **En cours d'exécution**.

- Dans la Web Console :

  - À l'aide du rapport *Rapport sur l'état des modules de l'application*. Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

  - Accédez à la section **Gestion des actifs** → **Actifs** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Général** → **Modules**.

    Le module Endpoint Detection and Response Optimum s'affiche avec l'état **En cours d'exécution**.

Cloud Sandbox

Cloud Sandbox est une technologie qui vous permet de détecter les menaces avancées sur les ordinateurs. Kaspersky Endpoint Security transmet automatiquement les fichiers détectés à Cloud Sandbox pour analyse. Cloud Sandbox exécute ces fichiers dans un environnement isolé pour détecter les activités malveillantes et prend des décisions concernant la réputation de ces fichiers. Les données de ces fichiers sont ensuite envoyées à Kaspersky Security Network. Par conséquent, si Cloud Sandbox a détecté un fichier malveillant, Kaspersky Endpoint Security effectuera l'action appropriée pour éliminer cette menace sur tous les ordinateurs où ce fichier est détecté.

Pour que Cloud Sandbox fonctionne, vous devez activer l'utilisation de Kaspersky Security Network.

Si vous utilisez Kaspersky Private Security Network, la technologie Cloud Sandbox n'est pas disponible.

La technologie Cloud Sandbox est toujours activée et disponible pour tous les utilisateurs de Kaspersky Security Network, quel que soit le type de licence que vous utilisez. Si vous avez déjà déployé la solution Endpoint Detection and Response Optimum, vous pouvez activer un compteur distinct pour les menaces détectées par Cloud Sandbox. Vous pouvez utiliser ce compteur pour compiler des statistiques lors de l'analyse des menaces détectées. Kaspersky Endpoint Security indique la technologie de détection des menaces Cloud Sandbox dans le *Rapport sur les menaces* de la console Kaspersky Security Center.

Comment activer le compteur Cloud Sandbox dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Sélectionnez l'onglet **Cloud Sandbox**.
6. Activez le commutateur **Cloud Sandbox ACTIVÉ**.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Detection and Response Expert (on-premises) est une solution de cybersécurité pour entreprises qui permet de se protéger contre la plupart des risques de cybersécurité et couvre les principaux scénarios de propagation des menaces. Les modules de Kaspersky Endpoint Detection and Response Expert (on-premises) sont déployés sur la plateforme de gestion unique Open Single Management Platform (OSMP). Pour plus d'informations sur la solution et la plateforme, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

L'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises) est assurée par le module de l'application Kaspersky Endpoint Security, Endpoint Detection and Response Expert (on-premises) (ci-après également dénommé *EDR Expert (on-premises)*).

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Fonctionnement d'Endpoint Detection and Response Expert (on-premises)

1. **Les appareils équipés de Kaspersky Endpoint Security établissent des connexions sécurisées avec le serveur d'actions de réponse aux menaces OSMP et le serveur de collecte de données télémétriques OSMP**
2. **Kaspersky Endpoint Security envoie les données au serveur de collecte de données télémétriques de la plateforme OSMP**

   Les informations suivantes sont transmises :

   - Informations sur les événements survenus sur l'appareil
   - Informations sur les menaces détectées par l'application
   - Informations sur les résultats du traitement de ces menaces
   - Données de surveillance relatives aux processus, aux connexions réseau ouvertes et aux fichiers modifiés

3. **Kaspersky Endpoint Security exécute des actions de réponse aux menaces**

   Les actions de réponse sont exécutées sur commande du serveur d'actions de réponse aux menaces de la plateforme OSMP.

Configuration de l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Conditions préalables

Avant de configurer l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) :

- Autorisez la connexion sur les ports 443 et 8443.
- Activez le module Détection comportementale pour transmettre les données télémétriques nécessaires.

  Si vous souhaitez obtenir des informations sur les menaces détectées par d'autres modules de protection, activez ces modules :

  - Protection contre les fichiers malicieux.
  - Protection contre les menaces réseau.
  - Protection contre les menaces Internet.
  - Protection contre le chiffrement.
  - Contrôle des applications.
  - Contrôle des appareils.
  - Contrôle de l'intégrité du système.

  > Lorsque vous utilisez le mécanisme eBPF pour obtenir la télémétrie du système dans le module Détection comportementale (disponible sur les systèmes d'exploitation 64 bits avec la version de noyau 4.18 et supérieure avec prise en charge eBPF), les données de télémétrie seront plus complètes.

- Ajoutez la clé de licence EDR Expert (on-premises) à l'application si vous avez acheté une licence distincte pour utiliser cette fonctionnalité.

  Si vous utilisez Kaspersky Endpoint Security sous une licence qui inclut Kaspersky Endpoint Detection and Response Expert (on-premises), aucune action n'est requise.

  Si l'application est utilisée en mode Light Agent, la clé de licence EDR Expert (on-premises) est ajoutée à la SVM.

- Vous devez également configurer un collecteur, un corrélateur et un stockage sur la plateforme OSMP.

Étapes essentielles de la configuration

1. **Obtenir et traiter les certificats émis par les serveurs OSMP**

   Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), les appareils exécutant Kaspersky Endpoint Security établissent des connexions HTTPS chiffrées avec le serveur d'actions de réponse aux menaces OSMP et le serveur de télémétrie OSMP.

Si l'utilisation d'un serveur proxy est configuré dans les paramètres généraux de l'application Kaspersky Endpoint Security, il est utilisé pour se connecter aux serveurs OSMP.

Les certificats permettant de sécuriser les connexions aux serveurs OSMP sont fournis par l'administrateur de la plateforme OSMP.

Pour traiter les certificats, suivez les étapes décrites dans l'article Conversion d'un certificat PFX au format PEM.

Vous pouvez utiliser un certificat de serveur et/ou un certificat client. Ce choix est déterminé par la stratégie de sécurité de votre organisation.

2. **Configurer les paramètres de l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Vous pouvez la configurer :

   - À l'aide de la Web Console (console Kaspersky Security Center et/ou Console OSMP).
   - À l'aide de la ligne de commande.

   Si vous souhaitez utiliser la Prévention de l'exécution des objets, vous pouvez activer les règles de prévention de l'exécution des objets du module EDR Expert (on-premises).

3. **Vérifier que la connexion à la plateforme Endpoint Detection and Response Expert (on-premises) a bien été établie**

   Vérifiez l'état d'EDR Expert (on-premises) de la manière qui vous convient.

4. **Gérer les paramètres supplémentaires si nécessaire**

   - Si SELinux est configuré en mode Enforcing sur votre système d'exploitation, vous devrez également configurer SELinux pour exécuter des actions de réponse.
   - Pour exécuter l'action de réponse **Vidage de la mémoire** ou **Vidage du processus**, débloquez ptrace.
   - Passez en revue les limitations de l'isolation du réseau.
   - Activez la transmission des informations sur les événements des applications tierces sur les appareils administrés. Pour ce faire, exécutez la commande suivante sur l'appareil administré :

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     L'activation de ce paramètre peut augmenter considérablement la charge du système d'exploitation.

Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premises)

Avant de préparer l'image, assurez-vous que le fichier `/var/opt/kaspersky/.ids_generated` n'existe pas sur l'appareil de référence.

Pour préparer une image de référence en vue d'une intégration correcte avec Kaspersky Endpoint Detection and Response Expert (on-premises) :

Ne redémarrez pas l'appareil de référence ni l'application Kaspersky Endpoint Security pendant que vous suivez ces instructions.

1. Exécutez les commandes suivantes en tant que root :

```
systemctl stop kesl
systemctl edit kesl
```

2. Dans l'éditeur, ajoutez l'une des configurations suivantes entre les lignes `### Anything between here and the comment below will become the contents of the drop-in file` et `### Edits below this comment will be discarded` :

   - Mettez à jour le SensorID à chaque démarrage de l'application sur les machines virtuelles temporaires

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - Mettez à jour le SensorID une seule fois sur les machines virtuelles persistantes

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. Enregistrez vos modifications et fermez l'éditeur.

   Le fichier `/etc/systemd/system/kesl.d/override.conf` est créé. Vérifiez son contenu pour vous assurer qu'il correspond à la configuration ajoutée.

4. Rechargez le service systemd en exécutant la commande suivante :

```
systemctl daemon-reload
```

5. Créez le fichier `/usr/bin/uuid-regen.sh` avec le contenu suivant :

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ---------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode ----------------------------------------------
MODE="a"
# ----- parse command-line arguments ------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file -----------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini ---------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. Modifiez les autorisations du fichier `/usr/bin/uuid-regen.sh` à l'aide de la commande suivante :

```
chmod 700 /usr/bin/uuid-regen.sh
```

L'appareil de référence est maintenant prêt pour la création de l'image du système d'exploitation.

Comment configurer l'intégration d'EDR Expert (on-premises)

Dans Web Console, vous pouvez activer ou désactiver le module EDR Expert (on-premises) et configurer l'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises) dans les propriétés de la stratégie de Kaspersky Endpoint Security.

Comment configurer l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Configuration des agents intégrés → Endpoint Detection and Response Expert (on-premises)**.
5. Sélectionnez l'option **Endpoint Detection and Response Expert version 8.0 ou ultérieure**.
6. Ajoutez des serveurs de collecte de données télémétriques et des serveurs de réponse.

   Pour ce faire, dans les sections **Connexion aux serveurs de collecte de données télémétriques** et **Connexion aux serveurs de réponse aux menaces**, cliquez sur le bouton **Ajouter**. Dans la fenêtre qui s'ouvre, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.
7. Ajoutez des certificats en cliquant sur le lien **Paramètres de connexion** dans les sections **Connexion aux serveurs de collecte de données télémétriques** et **Connexion aux serveurs de réponse aux menaces** ; puis, dans le volet qui s'affiche, effectuez les actions suivantes :

   a. Ajoutez un certificat de serveur en cliquant sur le bouton **Télécharger** dans la section correspondante.

   b. Si vous avez besoin d'une protection supplémentaire, créez un conteneur crypto.

      Pour ce faire, dans la section **Protection supplémentaire de la connexion** :

      1. Cochez la case **Utiliser l'authentification bidirectionnelle**.
      2. Cliquez sur le bouton **Télécharger** et ajoutez le certificat client que vous avez reçu lorsque vous avez terminé le scénario d'intégration principal.
      3. Saisissez le mot de passe du conteneur crypto dans le champ correspondant.

         Le champ **Mot de passe du conteneur crypto** est obligatoire. Vous ne pouvez pas enregistrer les paramètres sans saisir le mot de passe du certificat client (conteneur crypto).
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) via la ligne de commande

1. Pour ajouter un certificat de serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

2. Pour ajouter un certificat de serveur de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

3. Pour configurer les paramètres d'intégration, exécutez la commande suivante :

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Les paramètres et leurs valeurs possibles sont répertoriés dans le tableau ci-dessous.

4. Pour ajouter un certificat client pour la connexion au serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. Pour ajouter un certificat client pour la connexion au serveur de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. Pour activer l'intégration avec EDR Expert (on-premises), exécutez la commande suivante :

```
kesl-control --start-task 24
```

Paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security interagit avec des serveurs de la plateforme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` est le mode d'intégration d'EDR Expert (on-premises). Active l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur d'actions de réponse OSMP. Si l'authentification bidirectionnelle est activée sur le serveur de réponse aux menaces OSMP, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur d'actions de réponse aux menaces OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence d'envoi des requêtes de synchronisation au serveur de réponse OSMP (en minutes).	Valeur par défaut : `5`.
`ConnectionTimeout`	Délai d'expiration maximal de la connexion au serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`RequestTimeout`	Délai d'attente maximal d'une réponse du serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`EnableTelemetry`	Envoi des données relatives aux événements sur les appareils (télémétrie) au serveur de collecte de télémétrie OSMP.	`Yes` (valeur par défaut) : envoyer la télémétrie au serveur de collecte de télémétrie OSMP. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur d'actions de réponse OSMP. Vous pouvez ajouter plusieurs serveurs.		

Paramètre	Description	Valeur
`Address`	Adresse du serveur d'actions de réponse OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur d'actions de réponse OSMP.	Valeur par défaut : `443`.
La section **[TelemetrySettings]** contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.		
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur de collecte de télémétrie OSMP. Si l'authentification bidirectionnelle est activée sur le serveur de télémétrie OSMP, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur de télémétrie OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur de collecte de télémétrie OSMP en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente d'une réponse du serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `10`.
`OnlyTaggedEvents`	Envoi de la télémétrie avec IOA uniquement. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements.	`Yes` : envoyer uniquement les données de télémétrie comportant un indicateur d'attaque (Indicator of Attack, IOA). `No` (valeur par défaut) : envoyer toutes la télémétrie.
La section **[TelemetrySettings.Endpoints.item_#]** contient l'adresse et le port du serveur de collecte de télémétrie OSMP. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur de collecte de télémétrie OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur de collecte de télémétrie OSMP.	Valeur par défaut : `443`.
La section **[TelemetrySettings.EventTransferSettings]** contient les paramètres de transfert des données vers le serveur de collecte de télémétrie OSMP.		
`MaximumDataTransferTime`	Délai maximal d'envoi des événements au serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `30`.
`UseRequestCountLimits`	Limitez le nombre de requêtes. Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Pour les paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), les

stratégies imbriquées dans la hiérarchie permettent de spécifier des valeurs indépendantes, même si tous les autres paramètres de la stratégie sont hérités.

Si l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) est activée dans la stratégie parent et que l'héritage des paramètres est activé dans la stratégie enfant, les paramètres d'intégration de la stratégie enfant sont également hérités par défaut et ne peuvent pas être modifiés. Si vous souhaitez configurer des paramètres d'intégration indépendants, sélectionnez **Utiliser des paramètres de connexion personnalisés** dans la liste déroulante. Les paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) peuvent alors être modifiés.

Si vous utilisez Web Console ou la ligne de commande, pour procéder à l'intégration avec Kaspersky Endpoint Detection and Response (on-premises), vous devez sélectionner le mode d'intégration EDR (on-premises) dans les paramètres du module EDR Expert (on-premises) :

- Si vous utilisez Web Console, sélectionnez **Endpoint Detection and Response Expert (version 8.0 et supérieures)** dans les paramètres de la stratégie. Pour configurer l'intégration avec Kaspersky Endpoint Detection and Response (on-premises) sur un appareil, dans Web Console, vous devez gérer les « cadenas » pour l'une ou l'autre version (version 8.0 et ultérieure, et version 7.1 et antérieure).

- Si vous utilisez la ligne de commande, définissez le paramètre `Mode=EDRExpertOnPrem` dans les paramètres de tâche.

Comment vérifier que l'intégration EDR Expert (on-premises) est opérationnelle

Comment tester le module EDR Expert (on-premises) :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

- Dans la Web Console.

  - Dans Kaspersky Security Center Console :

    À l'aide du rapport *Rapport sur l'état des modules de l'application*. Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

  - Dans la console OSMP :

    - À l'aide du rapport *Rapport sur l'état des modules de l'application*.

    - Accédez à la section **Gestion des actifs** → **Actifs**, puis sélectionnez l'onglet **Analyse et réponse**.

      L'appareil s'affiche dans la liste avec l'état de télémétrie **Activité normale**.

    - Accédez à la section **Recherche de menaces**.

      Les événements de télémétrie de l'appareil s'affichent dans la liste des événements.

Endpoint Detection and Response Expert (cloud)

L'intégration de Kaspersky Endpoint Security for Linux à Kaspersky Endpoint Detection and Response Expert (cloud) est temporairement indisponible. Il est prévu que cette fonctionnalité soit prise en charge d'ici fin 2026. Consultez régulièrement nos notes de mise à jour pour vous tenir informé des mises à niveau des applications et des nouvelles fonctionnalités.

Kaspersky Endpoint Security for Linux prend en charge l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* est une solution de cybersécurité d'entreprise basée sur le cloud qui comprend des applications Kaspersky permettant à une organisation de se défendre contre la plupart des types de cyberrisques et de faire face aux scénarios de propagation des menaces les plus importants. Les modules EDR Expert (cloud) sont déployés sur Open Single Management Platform (OSMP). Cette plateforme exécute des scénarios multiplateformes dans une interface unique et permet d'intégrer des applications Kaspersky avec des applications tierces dans un système de sécurité complet.

L'un des éléments centraux de la solution est *SIEM*. Le SIEM suit les événements provenant de tous les modules et les met en corrélation les uns avec les autres à l'aide de règles définies par le fournisseur et l'utilisateur. EDR Expert (cloud) examine les données télémétriques et les journaux reçus de l'infrastructure de l'entreprise pour détecter automatiquement les attaques et permet d'enquêter sur les incidents à l'aide d'un graphique d'enquête unifié qui combine tous les événements collectés dans EDR Expert (cloud), y compris les événements provenant des applications Kaspersky et des produits de sécurité informatique tiers.

Pour la réponse aux incidents avancés, EDR Expert (cloud) utilise des scénarios prédéfinis et définis par l'utilisateur. Vous pouvez également utiliser des actions de réponse à partir d'applications tierces et des scénarios de réponse qui impliquent plusieurs applications.

Outils de Threat Intelligence

Kaspersky Endpoint Detection and Response utilise les outils Threat Intelligence suivants :

- L'intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations concernant la réputation des fichiers et des adresses Internet.
- Base de données des menaces de Kaspersky Threats.
- L'infrastructure du service Cloud Kaspersky Security Network (ci-après également appelé "KSN"), qui donne accès à des informations en temps réel sur la réputation des fichiers, des sites Internet et des logiciels à partir de la base de connaissances de Kaspersky. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de protection et réduit la possibilité de faux positifs.

Principe de fonctionnement de la solution

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification.

Les informations (télémétrie) sur les événements survenus sur l'ordinateur sont envoyées au serveur EDR Expert (cloud). Dans ce cas, Kaspersky Endpoint Security envoie également aux serveurs de collecte de données télémétriques des informations sur les menaces détectées par l'application, ainsi que des informations sur les résultats du traitement de ces menaces.

L'intégration de EDR Expert (cloud) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la plateforme Open Single Management Platform (OSMP), y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Limitations d'EDR Expert (cloud)

- Kaspersky Endpoint Security ne prend pas en charge l'intégration avec EDR Expert (cloud) en mode Light Agent.
- EDR Expert (cloud) n'est pas disponible pour les appareils dotés d'un processeur Elbrus.
- EDR Expert (cloud) n'est pas pris en charge sur les appareils basés sur l'architecture Arm.
- EDR Expert (cloud) n'est pas disponible pour les ordinateurs exécutant des systèmes d'exploitation 64 bits.

Comment configurer l'intégration de l'agent intégré avec EDR Expert (cloud)

Pour intégrer la solution Kaspersky Endpoint Detection and Response Expert (cloud), vous devez activer le module Endpoint Detection and Response Expert (cloud) et configurer la connexion au serveur de collecte des données de télémétrie et au serveur de réponse.

Un *serveur de collection de télémétrie* est un serveur qui fait partie d'une solution SIEM et qui collecte, normalise, corrèle, analyse et stocke les informations relatives aux événements qui se produisent sur l'ordinateur.

Un *serveur de réponse* est un serveur pour la réception et l'analyse des données, l'étude du comportement d'objets et la publication des résultats.

Les modules *Endpoint Detection and Response (cloud)* et *Endpoint Detection and Response Expert (on-premises)* ne sont pas compatibles entre eux.

Conditions de fonctionnement d'EDR Expert (cloud)

Pour qu'EDR Expert (cloud) fonctionne, les conditions suivantes doivent être remplies :

- L'infrastructure Kaspersky Endpoint Detection and Response Expert (cloud) est disponible dans votre région. Pour en savoir plus sur la disponibilité de l'infrastructure EDR Expert (cloud) dans votre région, veuillez contacter le Support technique.
- La plateforme OSMP (Open Single Management Platform) est installée.
- Kaspersky Endpoint Security installé en mode standard.
- Kaspersky Endpoint Security est activé, et la fonctionnalité est couverte par la licence.
- Vous avez accepté les conditions du Contrat de traitement des données de Kaspersky Endpoint Detection and Response Expert (cloud).
- Le module Endpoint Detection and Response Expert (cloud) est activé.
- Le module Détection comportementale pour la transmission des données télémétriques nécessaires est activé.

  Si vous souhaitez obtenir des informations sur les menaces détectées par d'autres modules de protection, activez ces modules :

  - Protection contre les fichiers malicieux.
  - Protection contre les menaces réseau.
  - Protection contre les menaces Internet.
  - Protection contre le chiffrement.
  - Contrôle des applications.
  - Contrôle des appareils.
  - Contrôle de l'intégrité du système.

Étapes de l'intégration à EDR Expert (cloud)

La configuration de l'Intégration EDR Expert (cloud) comprend les étapes suivantes :

1. **Sélection d'un mode EDR Expert**

   Kaspersky Endpoint Security prend en charge deux modes EDR Expert : on-premises et cloud. Pour intégrer Kaspersky Endpoint Detection and Response Expert (cloud), vous devez activer le mode correspondant lors de l'installation de l'application. Par défaut, l'application utilise l'intégration Endpoint Detection and Response Expert (on-premises).

2. **Activation de Kaspersky Endpoint Detection and Response Expert (cloud)**

   Vous devez acheter une licence distincte pour Kaspersky Endpoint Detection and Response Expert (cloud).

La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response Expert (cloud). Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour Kaspersky Endpoint Detection and Response Expert (cloud).

La licence de la fonctionnalité autonome Endpoint Detection and Response Expert (cloud) est la même que celle de Kaspersky Endpoint Security.

Assurez-vous que la fonctionnalité EDR Expert (cloud) est couverte par votre licence et qu'elle fonctionne dans Kaspersky Security Center ou sur l'appareil protégé.

3. **Configuration des paramètres de connexion au serveur de collecte des données de télémétrie et au serveur de réponse**

Kaspersky Endpoint Detection and Response Expert (cloud) requiert une connexion de confiance entre Kaspersky Endpoint Security et deux serveurs : le serveur de collecte des données de télémétrie et le serveur de réponse. L'application reçoit automatiquement les adresses des serveurs et les certificats permettant d'établir une connexion de confiance une fois que vous avez accepté les conditions du contrat de Kaspersky Endpoint Detection and Response Expert (cloud) relatif au traitement des données. Ainsi, vous devez uniquement gérer les paramètres avancés de connexion aux serveurs : l'utilisation ou non d'un tunnel TCP et l'intervalle d'envoi d'une demande de synchronisation avec le serveur.

Comment configurer les paramètres supplémentaires de connexion de Kaspersky Endpoint Security à EDR Expert (cloud) dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (cloud)**.
5. Activez le module à l'aide du commutateur **Endpoint Detection and Response Expert (cloud) DÉSACTIVÉ**.
6. Si la stratégie actuelle est une stratégie enfant et que la stratégie parent interdit la modification des paramètres d'intégration d'EDR Expert (cloud) (« cadenas » fermé), vous pouvez configurer l'héritage des paramètres dans la section **Héritage** :

   - **Hériter des paramètres de connexion de la stratégie** (valeur par défaut). Les paramètres de connexion sont hérités de la stratégie parent. Vous ne pourrez pas modifier les paramètres.
   - **Utiliser des paramètres de connexion personnalisés**. Vous pouvez configurer les paramètres de connexion manuellement.
7. L'onglet **Serveur de réponse** affiche le nom de domaine complet et le port du serveur de réponse, qui sont récupérés automatiquement. Si la stratégie de sécurité de votre infrastructure ne vous permet pas de vous connecter directement aux serveurs d'EDR Experts (cloud), vous pouvez établir une connexion via un tunnel TCP :

   a. Cochez la case **Utiliser un tunnel TCP pour la réponse**.

   b. Indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au tunnel.

8. Si nécessaire, définissez la fréquence d'envoi des demandes de synchronisation au serveur dans le champ **Envoyer une demande de synchronisation au serveur toutes les (min.)**. Pendant la synchronisation, Kaspersky Endpoint Security reçoit les tâches de réponse aux menaces et envoie les résultats des tâches.

9. Rendez-vous dans l'onglet **Serveur de collecte de données télémétriques**.

10. Configurez les paramètres de connexion au serveur de collecte des données de télémétrie :

    a. Cliquez sur le lien **Modifier**.

    b. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez un serveur de collecte des données de télémétrie dans la liste. Le collecteur KUMA sert de serveur de collecte de données télémétriques dans EDR Expert (cloud). Pour en savoir plus, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

    Si une erreur se produit lors de la connexion au serveur de collecte de données télémétriques, sélectionnez un autre serveur. Si vous ne parvenez pas à vous connecter au serveur de collecte des données de télémétrie, veuillez contacter le Support technique.

    c. Si nécessaire, vous pouvez configurer une connexion au serveur de collecte de données télémétriques via un tunnel TCP, comme vous le feriez pour le serveur de réponse.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment afficher les informations du certificat en ligne de commande

1. Pour afficher les informations relatives à un certificat client, exécutez la commande suivante :

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. Pour afficher les informations relatives à un certificat serveur, exécutez la commande suivante :

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

Par conséquent, Kaspersky Endpoint Security affiche les informations du certificat comme suit :

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

Vérifiez l'état de fonctionnement du module en consultant le *Rapport sur l'état des modules de l'application*. Vous pouvez également consulter l'état du module sur l'appareil protégé.

Optimisation de la transmission des données de télémétrie d'EDR Expert (cloud)

Télémétrie est une liste d'événements qui se sont produits sur l'ordinateur protégé. Kaspersky Endpoint Security analyse les données de télémétrie et les envoie aux serveurs de collecte de données télémétriques lors de la synchronisation. Les événements de télémétrie arrivent presque continuellement sur le serveur. Kaspersky Endpoint Security lance la synchronisation avec le serveur lorsque l'une des conditions suivantes est remplie :

- L'intervalle de synchronisation est écoulé.
- Le nombre d'événements dans la mémoire tampon dépasse la limite supérieure.

Par conséquent, par défaut, l'application se synchronise toutes les 30 secondes ou chaque fois que la mémoire tampon contient 1 024 événements. Vous pouvez configurer le comportement de synchronisation dans la stratégie de Kaspersky Endpoint Security et sélectionner les valeurs optimales en fonction de la charge de votre réseau (voir les instructions ci-dessous).

S'il n'y a pas de connexion entre Kaspersky Endpoint Security et le serveur, l'application met les nouveaux événements en file d'attente. Lorsque la connexion est rétablie, Kaspersky Endpoint Security envoie les événements de la file d'attente au serveur dans le bon ordre. Pour éviter de surcharger le serveur, Kaspersky Endpoint Security peut ignorer certains événements. Pour cela, vous pouvez optimiser les paramètres de transmission des événements, par exemple, pour définir une valeur maximale d'événements par heure (voir les instructions ci-dessous).

Comment optimiser la transmission de la télémétrie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés → Endpoint Detection and Response Expert (cloud)**.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres de transmission des données**.
6. Assurez-vous que la case **Envoi des données télémétriques ACTIVÉ** est cochée.
7. Si nécessaire, activez la fonctionnalité **Envoyer la télémétrie avec l'IOA uniquement**. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements. Cette fonction est désactivée par défaut.
8. Si nécessaire, configurez les paramètres de synchronisation du serveur :

   - **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
   - **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.

9. Rendez-vous dans l'onglet **Limitation des demandes**.

10. Si nécessaire, désactivez la limitation des demandes à l'aide du commutateur **Limitation des demandes ACTIVÉE**.

    Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Cette option est désactivée par défaut.

11. Configurez les paramètres d'optimisation pour l'envoi d'événements au serveur :

    - **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.

    - **Pourcentage de la limite d'événement excédentaire (%)**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment optimiser la transmission de la télémétrie en ligne de commande

1. Pour activer l'envoi de la télémétrie, exécutez la commande suivante :

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. Pour configurer les paramètres de synchronisation avec le serveur, exécutez la commande suivante :

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Paramètre	Description
`EnableTelemetry`	Envoi des données relatives aux événements sur les appareils (télémétrie) au serveur de collecte de télémétrie OSMP. L'envoi de la télémétrie est activé par défaut (`Yes`).
`TelemetrySettings.OnlyTaggedEvents`	Envoi de la télémétrie avec IOA uniquement. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements. Par défaut, l'envoi de la télémétrie avec IOA uniquement est désactivé (`No`).
La section `[TelemetrySettings.EventTransferSettings]` contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.	

Paramètre	Description
`UseRequestCountLimits`	Limitation des demandes. Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Cette option est désactivée par défaut.
`MaximumDataTransferTime`	Délai maximal de transmission des événements (s.). L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
`MaximumNumberOfEventsInHour`	Nombre maximal d'événements par heure. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.
`EventLimitExceededPercentage`	Pourcentage de la limite d'événement excédentaire (%). L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

Comment configurer les exclusions de télémétrie d'EDR Expert (cloud)

Pour améliorer les performances et optimiser la transmission des données vers le serveur de collecte de données télémétriques, vous pouvez ajouter des exclusions de télémétrie. Par exemple, vous pouvez choisir de ne pas envoyer les données de communication réseau pour certaines applications.

L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte des données de télémétrie et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Pour créer une exclusion de télémétrie dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions générales**.
   Une fenêtre s'ouvre pour ajouter une règle d'exclusion de télémétrie.

7. Configurez la règle d'exclusion de télémétrie :

   a. Si nécessaire, modifiez l'état de la règle. Par défaut, la règle est activée.

   b. Saisissez un nom pour la règle.

   c. Sélectionnez l'action à effectuer lorsque la règle est déclenchée :

   - **Ne pas collecter**. L'événement filtré sera exclu des données télémétriques envoyées.
   - **Exclure l'IOA**. L'événement déclencheur de la règle IOA sera exclu des données télémétriques envoyées. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements.

   d. Si l'option **Exclure l'IOA** est sélectionnée, indiquez les règles IOA à ajouter aux exclusions :

   - **Tout exclure**. Quand la condition indiquée est remplie, l'application exclut de la télémétrie les événements générés sur la base de toutes les règles IOA.
   - **Exclure par GUID**. Spécifiez le GUID de la règle IOA. Vous pouvez spécifier plusieurs GUID en utilisant le séparateur « `,` ». Pour en savoir plus sur les règles IOA, veuillez consulter l'aide relative à EDR Expert (cloud).

   e. Indiquez les conditions de filtrage :

   Si nécessaire, vous pouvez créer des critères de filtrage complexes en ajoutant plusieurs conditions de filtrage et des groupes de conditions à l'aide des opérateurs **ET**, **OU** et **NON**. Vous pouvez également ajouter des conditions imbriquées et des groupes de conditions à un groupe de conditions.

8. Le cas échéant, sous **Tous les types d'événements**, ajoutez des exclusions de télémétrie par type d'événement.

   a. Cliquez sur le nom du type d'événement.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Configurer manuellement**.

   c. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'exclusion**.

   Une fenêtre s'ouvre pour ajouter une règle d'exclusion de télémétrie. Dans la règle d'exclusion de télémétrie, la condition de filtrage `EventType`, qui correspond au type d'événement, est déjà prédéfinie dans la règle.

   d. Indiquez les conditions de filtrage :

9. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

Comment exporter ou importer des filtres d'événements EDR Expert (cloud)

Vous pouvez exporter la liste des exclusions dans un fichier JSON. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'identifiants d'événements. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder les filtres d'événements ou pour migrer la liste vers un autre serveur.

L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte des données de télémétrie et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Pour exporter et importer les filtres d'événements dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.
6. Pour exporter les filtres d'événements, procédez comme suit :
   a. Cliquez sur **Exporter**.
   b. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
   c. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.
7. Pour importer les filtres d'événements, procédez comme suit :
   a. Cliquez sur **Importer**.
   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.
   c. Sélectionnez la méthode d'importation des règles de filtrage des événements : en les ajoutant aux règles existantes ou en supprimant les règles existantes et en les remplaçant par de nouvelles.
   d. Ouvrez le fichier.

8. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

    1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
    2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

       La fenêtre des propriétés de la stratégie s'ouvre.
    3. Sélectionnez l'onglet **Paramètres de l'application**.
    4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
    5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.
    6. Pour exporter les filtres d'événements, procédez comme suit :

        a. Cliquez sur **Exporter**.

        b. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

        c. Enregistrez le fichier.

           Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.
    7. Pour importer les filtres d'événements, procédez comme suit :

        a. Cliquez sur **Importer**.

        b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

        c. Sélectionnez la méthode d'importation des règles de filtrage des événements : en les ajoutant aux règles existantes ou en supprimant les règles existantes et en les remplaçant par de nouvelles.

        d. Ouvrez le fichier.
    8. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform est une solution de protection de l'infrastructure informatique d'une organisation et de détection précoce des menaces telles que les attaques zero-day, les attaques ciblées et les menaces persistantes avancées (ci-après également appelées APT). Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

L'application Kaspersky Endpoint Security peut s'intégrer aux modules suivants de Kaspersky Anti Targeted Attack Platform :

Kaspersky Endpoint Detection and Response (KATA)

Le module assure la protéction des appareils dans le réseau local de l'organisation. Lorsqu'il est intégré à Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security exécute les fonctions suivantes :

- Envoie les informations sur les événements sur les appareils (télémétrie) au serveur Central Node qui assure l'interaction avec Kaspersky Endpoint Detection and Response (KATA) (ci-après également appelé *serveur KATA*).

  Kaspersky Endpoint Security envoie au module Central Node des données de surveillance sur les processus, les connexions réseau ouvertes et les fichiers modifiés, ainsi que des données sur les menaces détectées par l'application et des données sur les résultats du traitement de ces menaces.

- Exécute les actions de réponse aux menaces pour garantir la sécurité lors de la réception de commandes de Kaspersky Anti Targeted Attack Platform.

L'intégration avec Kaspersky Endpoint Detection and Response (KATA) versions 7.1 et antérieures est prise en charge.

Network Detection and Response (KATA)

Le module assure la protection du réseau interne de l'organisation. Lorsqu'elle est intégrée à Kaspersky Network Detection and Response (KATA), l'application Kaspersky Endpoint Security peut envoyer des données sur les événements sur les appareils (télémétrie) à un serveur avec le module Central Node qui assure l'interaction avec Kaspersky Network Detection and Response (KATA) (ci-après également appelé *serveur NDR*).

Sandbox

L'application Kaspersky Endpoint Security envoie les fichiers à analyser au serveur Central Node qui gère l'interaction avec Bac à sable.

Les modules suivants de Kaspersky Endpoint Security permettent l'intégration avec Kaspersky Anti Targeted Attack Platform :

- Endpoint Detection and Response Expert (on-premises), ci-après également appelé *EDR Expert (on-premises)*.

  À partir de Kaspersky Endpoint Security 12.4 for Linux, le module Endpoint Detection and Response (KATA) a été renommé Endpoint Detection and Response Expert (on-premises). Ce module assure désormais l'intégration non seulement avec Kaspersky Endpoint Detection and Response (KATA), un module de Kaspersky Anti Targeted Attack Platform, mais aussi avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises).

- Network Detection and Response (KATA), ci-après également appelé *NDR (KATA)*.

- Sandbox.

Vous pouvez configurer l'intégration de l'application Kaspersky Endpoint Security avec tous les modules de la solution Kaspersky Anti Targeted Attack Platform ou avec chaque module séparément.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Configuration de l'intégration avec Kaspersky Anti Targeted Attack Platform

Conditions préalables

Avant de configurer l'intégration avec Kaspersky Network Detection and Response (KATA), autorisez la connexion sur le port 8085.

Avant de configurer l'intégration avec le module Kaspersky Endpoint Detection and Response (KATA) :

- Autoriser la connexion sur les ports 443, 8443.
- Activez le module Détection comportementale pour transmettre les données télémétriques nécessaires.

  > Le module Analyse comportementale est disponible sur les appareils dotés d'un noyau de version 3.13 ou ultérieure.

  Si vous souhaitez obtenir des informations sur les menaces détectées par d'autres modules de protection, activez ces modules :

  - Protection contre les fichiers malicieux.
  - Protection contre les menaces réseau.
  - Protection contre les menaces Internet.
  - Protection contre le chiffrement.
  - Contrôle des applications.
  - Contrôle des appareils.
  - Contrôle de l'intégrité du système.

  L'activation du mode d'interception du trafic réseau eBPF rend les données de télémétrie plus complètes. La technologie eBPF est disponible sur les ordinateurs exécutant un système d'exploitation 64 bits avec un noyau version 4.18 ou ultérieure prenant en charge eBPF.

  > Nous vous recommandons de vérifier si votre ordinateur prend en charge les modules requis pour l'envoi de la télémétrie.

- Ajoutez la clé de licence EDR Expert (on-premises) à l'application si vous avez acheté une licence distincte pour utiliser cette fonctionnalité.

  Si vous utilisez Kaspersky Endpoint Security sous une licence qui inclut Kaspersky Endpoint Detection and Response Expert (on-premises), aucune action n'est requise.

  > Si vous utilisez Kaspersky Endpoint Security en mode Light Agent, vous devez ajouter aux SVM la clé de licence pour activer la fonctionnalité supplémentaire.

Étapes essentielles de la configuration

1. **Obtenir et traiter les certificats émis par les serveurs Central Node**

   Lors de l'intégration avec la solution Kaspersky Anti Targeted Attack Platform, les appareils exécutant Kaspersky Endpoint Security établissent des connexions chiffrées HTTPS avec les serveurs hébergeant le module Central Node qui facilite l'intégration.

   > Si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application de Kaspersky Endpoint Security, il sera utilisé pour se connecter à ces serveurs.

   Les certificats permettant de sécuriser les connexions aux serveurs compatibles avec les modules de Kaspersky Anti Targeted Attack Platform sont fournis par l'administrateur de cette plateforme.

   Pour traiter les certificats, suivez les étapes décrites dans l'article Conversion d'un certificat PFX au format PEM.

   Vous pouvez utiliser un certificat de serveur et/ou un certificat client. Ce choix est déterminé par la stratégie de sécurité de votre organisation.

2. **Configurer les paramètres d'intégration avec Kaspersky Anti Targeted Attack Platform**

   Vous pouvez la configurer :

   - À l'aide de Web Console (EDR (KATA) et NDR (KATA) dans la console de Kaspersky Security Center et/ou dans la Console OSMP).
   - À l'aide de la Console d'administration de Kaspersky Security Center (EDR (KATA) et NDR (KATA)).
   - À l'aide de la ligne de commande (EDR (KATA) et NDR (KATA)).

3. **Vérifiez que la connexion à Kaspersky Anti Targeted Attack Platform a été établie avec succès.**

   Vérifiez l'état des modules de Kaspersky Anti Targeted Attack Platform de la manière qui vous convient.

4. **Gérer les paramètres supplémentaires si nécessaire**

   - Si SELinux est configuré en mode Enforcing sur votre système d'exploitation, vous devrez également configurer SELinux pour exécuter des actions de réponse.
   - Passez en revue les limitations de l'isolation du réseau.

Comment configurer l'intégration EDR (KATA)

Dans la Web Console, vous pouvez activer ou désactiver le module Kaspersky Endpoint Detection and Response (KATA) et configurer l'intégration de l'application Kaspersky Endpoint Security avec ce module.

Comment configurer l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la fenêtre des propriétés de la stratégie qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

5. Accédez à **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.

6. Dans la partie droite de l'écran :

   a. Sélectionnez l'option **Endpoint Detection and Response Expert version 7.1 ou antérieure**.

   b. Dans la section **Connexion aux serveurs de collecte de données télémétriques**, sélectionnez un serveur de collecte de données télémétriques en cliquant sur le bouton **Ajouter** dans la barre d'outils, puis cliquez sur **Sélectionner le serveur**.

   c. Dans la section **Connexion aux serveurs de réponse**, sélectionnez un serveur de réponse en cliquant sur le bouton **Ajouter** dans la barre d'outils, puis cliquez sur **Sélectionner le serveur**.

   d. Cliquez sur le lien **Paramètres de connexion** dans les sections **Connexion aux serveurs de collecte de données télémétriques** et **Connexion aux serveurs de réponse aux menaces**, puis, dans le volet qui s'affiche :

      1. Ajoutez un certificat de serveur en cliquant sur le bouton **Charger**.

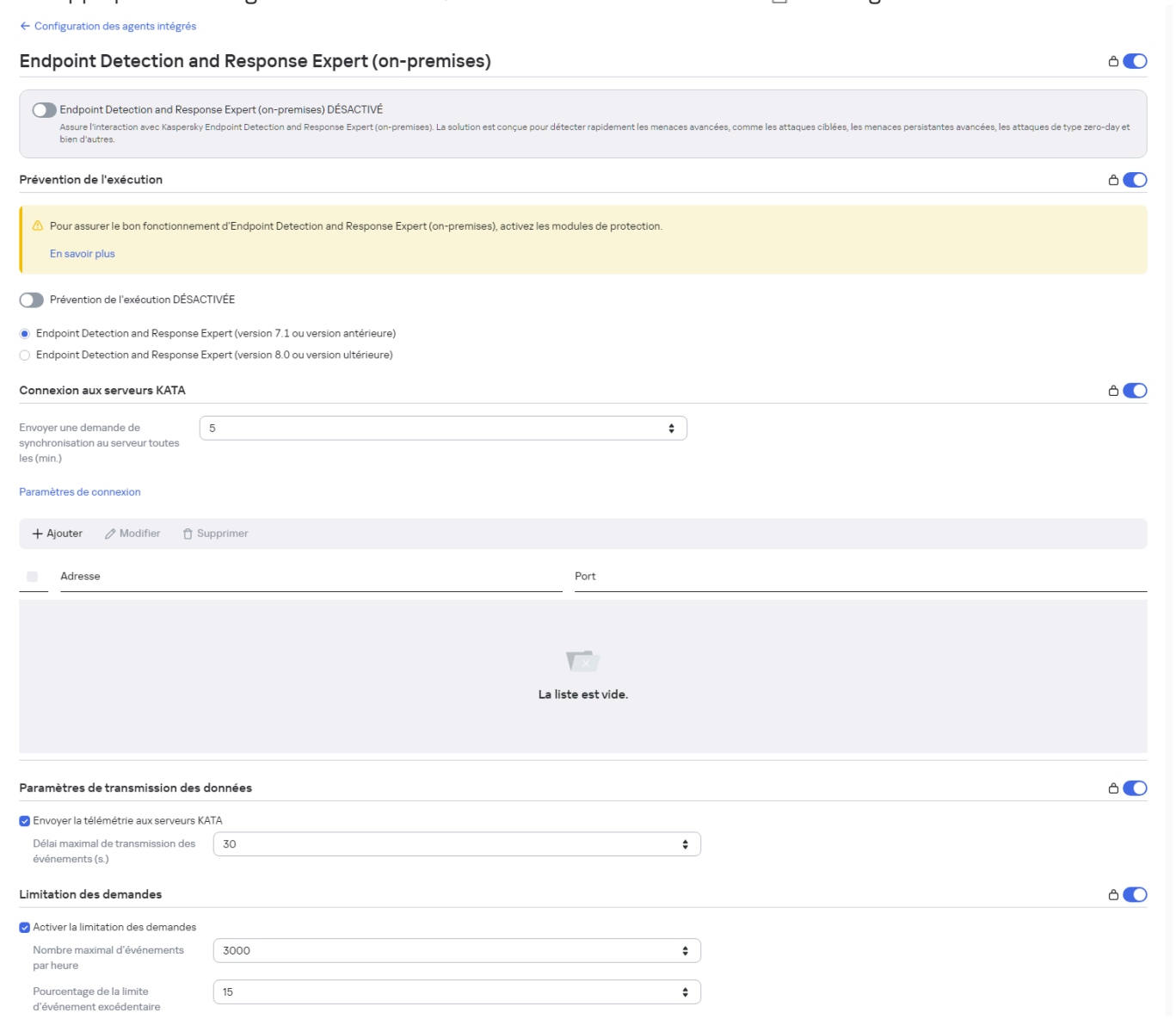
      2. Si vous avez besoin d'une protection supplémentaire, créez un conteneur crypto.

         Pour ce faire, dans la section **Protection supplémentaire de la connexion** :

         - Cochez la case **Utiliser l'authentification bidirectionnelle**.
         - Cliquez sur le bouton **Charger** et ajoutez le certificat client que vous avez obtenu à l'étape 1 du scénario principal.
         - Saisissez le mot de passe du conteneur crypto dans le champ correspondant.

         Le champ **Mot de passe du conteneur crypto** est obligatoire. Vous ne pouvez pas enregistrer les paramètres sans saisir le mot de passe du certificat client (conteneur crypto).

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Endpoint Detection and Response Expert (on-premises)

Comment configurer l'intégration avec Kaspersky Endpoint Detection and Response (KATA) en ligne de commande

1. Pour sélectionner un mode d'intégration EDR (KATA), exécutez la commande suivante :

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. Pour ajouter un serveur Central Node, exécutez la commande suivante :

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. Pour ajouter un certificat de serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. Pour configurer les paramètres d'intégration, exécutez la commande suivante :

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Les paramètres et leurs valeurs possibles sont répertoriés dans le tableau ci-dessous.

5. Pour ajouter un certificat client pour la connexion au serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. Pour activer l'intégration avec EDR (KATA), exécutez la commande suivante :

```
kesl-control --start-task 24
```

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security interagit avec des serveurs de la plateforme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` est le mode d'intégration d'EDR Expert (on-premises). Active l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. Si l'authentification bidirectionnelle est activée côté serveur KATA, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur KATA, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KATA en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur KATA en secondes.	Valeur par défaut : `10`.
`EnableTelemetry`	Envoi des données d'événement (télémétrie) à KATA.	`Yes` (valeur par défaut) : envoie la télémétrie au serveur KATA. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur KATA. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur KATA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur KATA.	Valeur par défaut : `443`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des données vers le serveur KATA.		

Paramètre	Description	Valeur
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur KATA.	Valeur par défaut : `30`.
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur KATA.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Si vous utilisez Web Console ou la ligne de commande, pour procéder à l'intégration avec Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration *EDR (KATA)* dans les paramètres du module EDR Expert (on-premises) :

- Si vous utilisez Web Console, sélectionnez l'option **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** dans les paramètres de la stratégie. Pour configurer l'intégration avec Kaspersky Endpoint Detection and Response (KATA) sur un appareil dans la Web Console, vous devez gérer les « cadenas » pour l'une ou l'autre version (version 8.0 et ultérieure et version 7.1 et antérieure).
- Si vous utilisez la ligne de commande, définissez le paramètre `Mode=EDRKATA` dans les paramètres de tâche.

Comment configurer l'intégration NDR (KATA)

Dans Web Console, vous pouvez activer ou désactiver le module Kaspersky Network Detection and Response (KATA) et configurer l'intégration de l'application Kaspersky Endpoint Security avec ce module.

Comment configurer l'intégration avec Kaspersky Network Detection and Response (KATA) dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Configuration des agents intégrés → Network Detection and Response (KATA)**.
5. Activez le commutateur **Network Detection and Response (KATA)**.
6. Cliquez sur **Paramètres de connexion**.
7. Configurez la connexion au serveur :
   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.
   - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

- **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

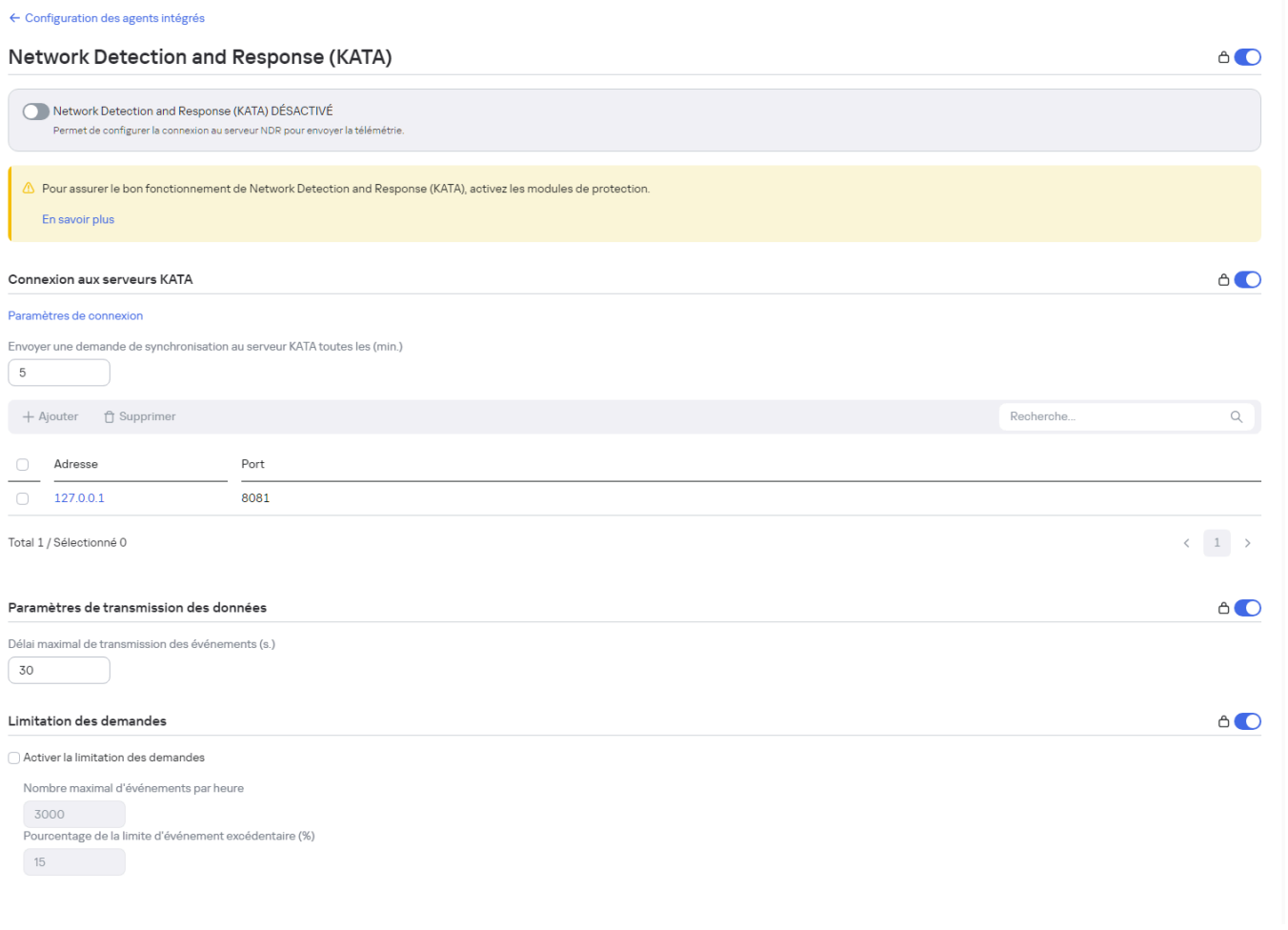
  Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

8. Cliquez sur **OK**.

9. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

10. Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Network Detection and Response (KATA)

Comment configurer l'intégration avec Kaspersky Network Detection and Response (KATA) dans la ligne de commande

1. Pour ajouter un serveur Central Node, exécutez la commande suivante :

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

2. Pour ajouter un certificat de serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. Pour configurer les paramètres d'intégration, exécutez la commande suivante :

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

Les paramètres et leurs valeurs possibles sont répertoriés dans le tableau ci-dessous.

4. Pour ajouter un certificat client pour la connexion au serveur de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. Pour activer l'intégration avec NDR (KATA), exécutez la commande suivante :

```
kesl-control --start-task 31
```

Paramètres de la tâche Intégration à Kaspersky Network Detection and Response (KATA)

Paramètre	Description	Valeur
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. Si l'analyse du certificat client est activée du côté serveur NDR, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)*.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur NDR en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur NDR en secondes.	Valeur par défaut : `10`.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur NDR.		
`Address`	Adresse du serveur NDR. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur NDR.	Valeur par défaut : `8081`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur NDR.		
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur NDR.	Valeur par défaut : `30`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.

Paramètre	Description	Valeur
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur NDR.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`EventLimitExceededPercentage`	Pourcentage de dépassement de la limite d'événements. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.
`PingPeriod`	Fréquence d'interrogation des serveurs NDR en secondes.	Valeur par défaut : `450`.

Comment vérifier que l'Intégration KATA est opérationnelle

Vous pouvez tester les modules de Kaspersky Anti Targeted Attack Platform des manières suivantes :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

  Pour l'intégration aux modules EDR (on-premises) et NDR (KATA), l'état **Disponible et en cours d'exécution** s'affiche.

- Dans la Web Console :

  - Dans la console Kaspersky Security Center, à l'aide du rapport *Rapport sur l'état des modules de l'application*. Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

  - Dans la console OSMP :

    - À l'aide du rapport *Rapport sur l'état des modules de l'application*.

    - Accédez à la section **Gestion des actifs** → **Actifs**, puis sélectionnez l'onglet **Analyse et réponse**.

      L'appareil s'affiche dans la liste avec l'état de télémétrie **Activité normale**.

    - Accédez à la section **Chasse aux menaces**.

      Les événements de télémétrie de l'appareil s'affichent dans la liste des événements.

- Dans Kaspersky Anti Targeted Attack Platform :

  Accédez à la section **Actifs** → **Appareils**. Les appareils s'affichent dans le tableau. Si nécessaire, vous pouvez filtrer le tableau par **application EPP**, **connexion EPP** et **dernière connexion à EPP**.

  Un clic sur le nom d'un appareil ouvre un volet. Dans la section **Agent Endpoint**, l'état de la connexion est **Actif**.

Sandbox

La technologie Sandbox permet l'analyse et l'exploration des objets sur des serveurs dédiés, dotés d'images virtuelles de systèmes d'exploitation, afin de détecter les activités malveillantes et les signes d'attaques ciblées sur l'infrastructure informatique de l'organisation.

L'application Kaspersky Endpoint Security peut interagir avec Sandbox via Open Single Management Platform (OSMP) ou Kaspersky Anti Targeted Attack Platform.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Comment configurer l'intégration avec Sandbox

Avant de commencer à configurer l'intégration avec Sandbox :

- Autorisez les connexions entrantes et sortantes comme suit :
  - Entrant (interface d'administration) :
    - TCP 22
    - TCP 443
    - TCP 8443
  - Sortant (interface d'administration) :
    - TCP 80 ou TCP 443
  - Sens sortant et sens entrant correspondant (interface d'accès aux objets traités) :

    N'importe quel port.
- Installez l'interface graphique (paquet kesl-gui) si vous souhaitez envoyer manuellement des fichiers vers Sandbox depuis le menu contextuel d'un fichier ou d'un répertoire.

Étapes essentielles de la configuration

1. **Créez une demande de connexion au serveur Sandbox sur la plateforme, puis confirmez la connexion dans la console d'administration de Sandbox**

   Pour en savoir plus, consultez l'aide des solutions correspondantes :

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   Enregistrez l'adresse IP du serveur Sandbox de la manière qui vous convient. Vous en aurez besoin pour la configuration ultérieure de l'intégration.
2. **Obtenir et traiter les certificats émis par le serveur OSMP ou le serveur Nœud central**

Lors de l'intégration avec Sandbox, les appareils exécutant Kaspersky Endpoint Security établissent des connexions chiffrées via HTTPS avec les Serveurs d'intégration.

Si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application Kaspersky Endpoint Security, le serveur proxy est utilisé pour se connecter aux serveurs qui assurent l'interaction avec Sandbox.

Les certificats permettant de sécuriser les connexions aux serveurs autorisant l'interaction avec Sandbox sont fournis par l'administrateur de OSMP ou Kaspersky Anti Targeted Attack Platform.

Pour traiter les certificats, suivez les étapes décrites dans l'article Conversion d'un certificat PFX au format PEM.

Vous pouvez utiliser un certificat de serveur et/ou un certificat client. Ce choix est déterminé par la stratégie de sécurité de votre organisation.

3 Gérer les paramètres de l'intégration avec Sandbox

Pour envoyer des fichiers à l'analyse, vous devez activer l'intégration avec KATA Sandbox et ajouter un serveur Central Node qui est déployé au sein de la solution.

Comment configurer l'intégration avec Sandbox dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés → Sandbox**.
5. Dans la liste déroulante **Type d'envoi de fichiers pour analyse**, sélectionnez la méthode requise :

   - **Manuel**. Dans ce mode, vous pouvez envoyer des objets à Sandbox pour analyse manuellement à l'aide d'une commande ou depuis le menu contextuel **Vérifier dans Sandbox**.

     Nous vous recommandons de sélectionner ce type si votre version de Sandbox est antérieure à 8.0.

   - **Automatique**. L'application soumet automatiquement les objets pour analyse, mais il n'est pas possible de soumettre manuellement les objets pour analyse à Sandbox.

   - **Combiné**. L'application soumet automatiquement les objets pour analyse, mais vous pouvez également les soumettre manuellement à Sandbox à l'aide d'une commande ou via l'interface graphique.
6. Dans la section **Connexion aux serveurs Sandbox** :

   - Ajoutez le Serveur d'intégration en cliquant sur le bouton **Ajouter** dans la barre d'outils.

     Vous pouvez indiquer l'adresse IP de la plateforme KATA / OSMP ou son FQDN comme adresse.

     Si le serveur Sandbox est connecté à OSMP, vous pouvez uniquement indiquer le FQDN du serveur d'agent.

- Ajoutez le certificat de serveur de Kaspersky Anti Targeted Attack Platform ou d'OSMP que vous avez reçu à l'étape 2 du scénario principal.

  Pour ce faire, cliquez sur le lien **Paramètres de connexion au serveur**, puis, dans le volet qui s'affiche, dans la section **Certificat TLS du serveur**, cliquez sur le bouton **Charger**.

- Si vous avez besoin d'une protection supplémentaire, créez un conteneur crypto.

  Pour ce faire, dans la section **Sécurité supplémentaire des connexions** :

  - Cochez la case **Utiliser l'authentification bidirectionnelle**.
  - Cliquez sur le bouton **Charger** et ajoutez un certificat client.
  - Saisissez le mot de passe du conteneur crypto dans le champ correspondant.

  Le champ **Mot de passe du conteneur crypto** est obligatoire. Vous ne pouvez pas enregistrer les paramètres sans saisir le mot de passe du certificat client (conteneur crypto).

7. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

   - **Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer un objet, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où vous auriez besoin ultérieurement de restaurer l'objet. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.
   - **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security vérifie la mémoire du noyau, les processus en cours d'exécution et les secteurs de démarrage.
   - **Créer la tâche Analyse IOC**. Si cette option est sélectionnée, Kaspersky Endpoint Security crée automatiquement la tâche *Analyse IOC (tâche autonome d'analyse IOC)*. Pour cette tâche, vous pouvez configurer le mode d'exécution, la zone d'analyse et l'action en cas de détection d'un IOC (*Placer la copie en Quarantaine, supprimer l'objet* ou *Lancer l'Analyse des zones critiques*). Pour modifier les autres paramètres de la tâche *Analyse IOC*, accédez aux paramètres de la tâche.

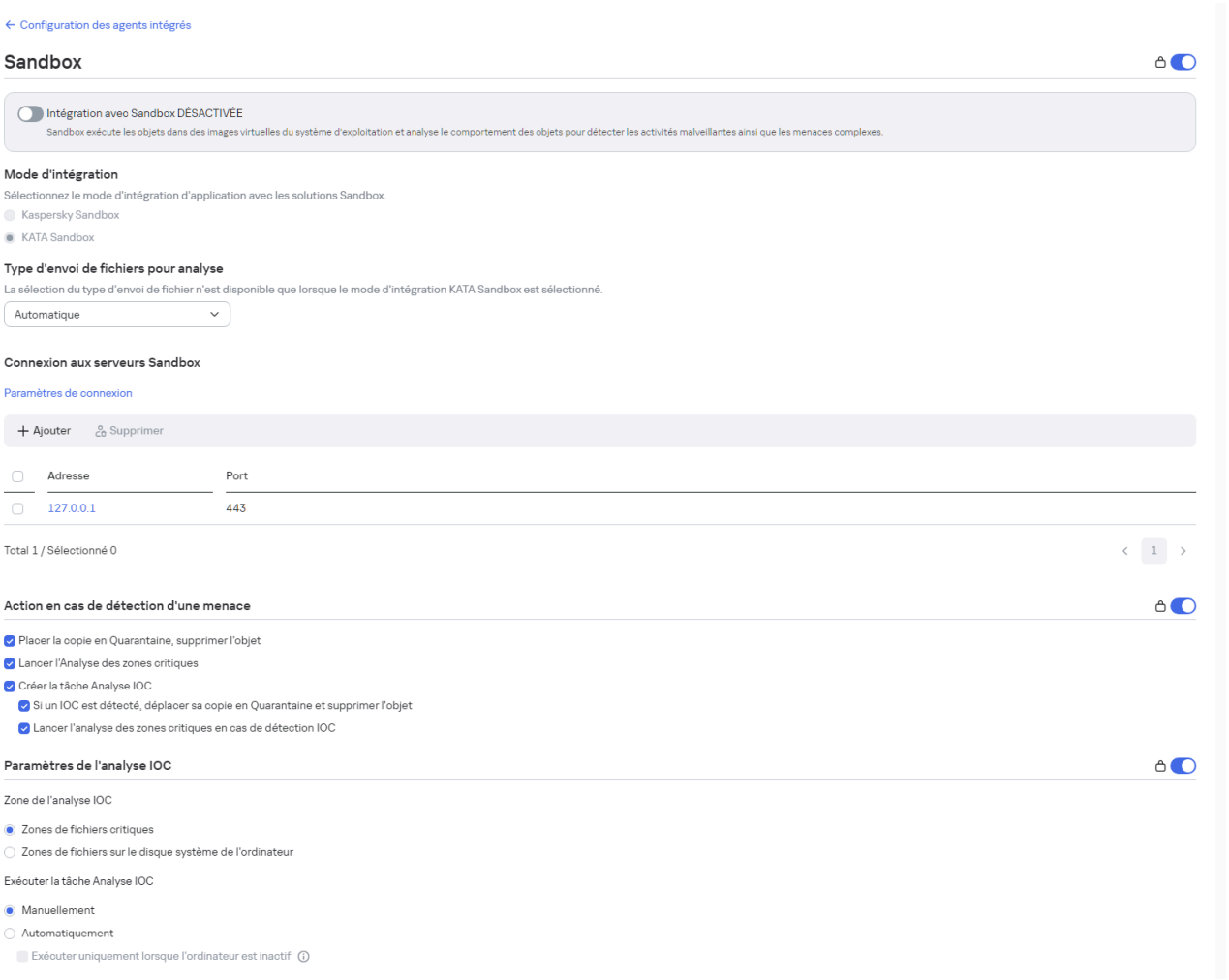
8. Si nécessaire, configurez les paramètres de la tâche *Analyse IOC* dans le groupe **Zone de l'analyse IOC**.

   - **Zones de fichiers critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security recherche des IOC uniquement dans les répertoires utilisateur et système.
   - **Zones de fichiers sur le disque système de l'ordinateur**. Si cette option est sélectionnée, Kaspersky Endpoint Security analyse tous les fichiers du système de fichiers racine à la recherche d'IOC.

9. Si nécessaire, configurez les paramètres de la tâche *Analyse IOC* dans le groupe **Exécuter la tâche Analyse IOC**.

   - **Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer la tâche *Analyse IOC* manuellement à tout moment.
   - **Automatiquement**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute automatiquement la tâche *Analyse IOC* après la détection d'une menace.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Sandbox

Comment configurer l'intégration avec Sandbox en ligne de commande

1. Pour ajouter un certificat de serveur, exécutez la commande suivante :

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. Pour ajouter un serveur Nœud central ou OSMP, exécutez la commande suivante :

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. Pour configurer les paramètres d'intégration, exécutez la commande suivante :

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

Les paramètres et leurs valeurs possibles sont répertoriés dans le tableau ci-dessous.

4. Pour ajouter un certificat client, exécutez la commande suivante :

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. Pour activer l'intégration avec Sandbox, exécutez la commande suivante :

```
kesl-control --start-task 29
```

Paramètres de la tâche Intégration avec Sandbox

Paramètre	Description	Valeur
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. Si la vérification du certificat client est activée du côté serveur Sandbox, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Sandbox*.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur en secondes.	Valeur par défaut : `10`.
`SendingMode`	Mode d'envoi du fichier pour analyse à Sandbox.	`AutoOnly` (valeur par défaut) : envoi automatiquement des fichiers pour analyse dès qu'ils sont consultés. `Manual` : envoi manuel des fichiers pour analyse. `AutoAndManual` : envoi des fichiers à analyser, que ce soit automatique ou manuel.
`QuarantineFile`	Place un fichier en quarantaine lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : en cas de menace détectée, supprimer le fichier original et mettre la copie en quarantaine. `No` : ne pas placer le fichier en quarantaine en cas de menace détectée.
`ScanCriticalAreas`	Exécution de l'analyse des zones critiques en cas de menace détectée.	`Yes` (valeur par défaut) : lorsqu'une menace est détectée, effectuer une analyse des zones critiques. `No` : ne pas lancer d'analyse des zones critiques lorsqu'une menace est détectée.
`CreateIocScanTask`	Créer une tâche d'analyse IOC lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : créer une tâche d'analyse IOC lorsqu'une menace est détectée. `No` : ne pas créer de tâche d'analyse IOC lorsqu'une menace est détectée.
`QuarantineFileOnIocDetected`	Mise en quarantaine d'un objet lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, supprimer l'objet original et mettre en quarantaine la copie de l'objet. `No` : ne pas mettre l'objet en quarantaine lorsqu'un indicateur de compromission est détecté.
`ScanCriticalAreasOnIocDetected`	Exécution de l'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, exécuter une analyse des zones critiques. `No` : ne pas exécuter d'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.
`Drives`	Domaines de recherche d'indicateurs de compromission.	`Critical` (valeur par défaut) : vérifier les fichiers dans les répertoires utilisateur et système. `System` : analyser tous les fichiers du système de fichiers racine.

Paramètre	Description	Valeur
`ScheduleMode`	Mode de lancement de la tâche d'analyse IOC.	`Manually` (valeur par défaut) : exécuter manuellement la tâche d'analyse IOC. `AfterTreatDetected` : exécuter la tâche d'analyse IOC après la détection d'une menace.
La section **[Servers.item_#]** contient les paramètres du serveur Sandbox.		
`Address`	Adresse du serveur. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur.	Valeur par défaut : `443`.
La section **[SandboxTransferSettings]** contient les paramètres de transfert des fichiers à analyser dans Sandbox.		
`SandboxQueue`	Taille maximale du répertoire de stockage de la file d'attente des demandes d'analyse en mégaoctets.	Valeur par défaut : `1024`.

4. **Vérifiez que la connexion à Sandbox a bien été établie**

   Vérifiez l'état de Sandbox de la manière qui vous convient.

Comment vérifier que l'intégration avec Sandbox est opérationnelle

Vous pouvez tester le module Sandbox des manières suivantes :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

  L'intégration avec Sandbox s'affiche avec l'état **Disponible et en cours d'exécution**.

- Dans la Web Console :

  - Dans Kaspersky Security Center Console :

    À l'aide du rapport *Rapport sur l'état des modules de l'application*. Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

  - Dans la console OSMP :

    - À l'aide du rapport *Rapport sur l'état des modules de l'application*.
    - Accédez à la section **Chasse aux menaces**.

      Les événements de connexion réussie à Sandbox s'affichent dans la liste des événements.

- Dans Kaspersky Anti Targeted Attack Platform :

  Accédez à la section **Actifs** → **Appareils**. Les appareils s'affichent dans le tableau. Si nécessaire, vous pouvez filtrer le tableau par **application EPP**, **connexion EPP** et **dernière connexion à EPP**.

  Un clic sur le nom d'un appareil ouvre un volet. Dans la section Endpoint Agent, l'état de connexion est **Actif**.

Comment envoyer manuellement un fichier à Sandbox

Kaspersky Endpoint Security permet aux utilisateurs d'envoyer manuellement des fichiers ou des répertoires pour analyse dans Sandbox depuis le menu contextuel.

Pour envoyer des fichiers pour analyse dans Sandbox, les conditions suivantes doivent être remplies :

- L'interface graphique de Kaspersky Endpoint Security doit être installée.
- Kaspersky Endpoint Security doit être intégré à Sandbox.
- Le mode d'envoi des fichiers pour analyse doit être défini sur **Manuel** ou **Combiné**.

Pour envoyer un fichier ou un répertoire à analyser dans Sandbox :

1. Ouvrez le menu contextuel du fichier ou du répertoire que vous souhaitez analyser.
2. Sélectionnez **Kaspersky Endpoint Security 12.5 for Linux** comme application pour ouvrir le fichier ou le répertoire.

   Les noms des éléments du menu contextuel peuvent varier en fonction de votre environnement de bureau.

3. Ensuite, dans le menu contextuel, sélectionnez **Vérifier dans Sandbox**.

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security inclut un agent intégré pour l'intégration à la solution Kaspersky Managed Detection and Response. La solution *Kaspersky Managed Detection and Response (MDR)* détecte et analyse automatiquement les incidents de sécurité dans votre infrastructure. Pour ce faire, MDR utilise les données de télémétrie reçues des terminaux et Machine learning. MDR envoie les données de l'incident aux experts de Kaspersky. Les experts peuvent alors traiter l'incident et, par exemple, ajouter une nouvelle entrée dans les bases antivirus. Les experts peuvent également émettre des recommandations sur le traitement de l'incident et, par exemple, suggérer d'isoler l'ordinateur du réseau. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Managed Detection and Response.

L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Managed Detection and Response (ci-après également appelé MDR). Le module doit être activé de l'une des manières décrites dans le scénario d'intégration.

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Configurations de Kaspersky Endpoint Security pour l'intégration avec MDR

Les configurations suivantes peuvent être appliquées pour utiliser MDR :

- **[KES+agent intégré]**. Dans cette configuration, Kaspersky Endpoint Security agit à la fois comme une application assurant la sécurité de l'ordinateur et comme une application permettant d'utiliser MDR.
- **[PPE tierce+EDR Agent]**. Dans cette configuration, la sécurité de l'infrastructure informatique est assurée par la Endpoint Protection Platform (PPE) tierce. L'interaction avec MDR est assurée par Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent (EDR Agent). Dans cette configuration, EDR Agent est compatible avec les applications EPP tierces.

Recommandations pour la création d'une image de référence en vue d'une intégration correcte avec MDR

Nous ne recommandons pas d'inclure l'application Kaspersky Endpoint Security for Linux dans l'image de référence.

Si Kaspersky Endpoint Security for Linux a été inclus dans l'image de référence, procédez comme suit sur chaque appareil basé sur cette image :

1. Pour créer une tâche, exécutez la commande suivante :
2. Désinstallez Kaspersky Endpoint Security for Linux, puis réinstallez-le.

Si vous ne suivez pas ces étapes, il se peut que les appareils ne soient pas identifiés correctement.

Chargement du fichier de configuration KPSN

Si votre configuration ne répond pas aux exigences de fonctionnement sans fichiers de configuration KPSN, vous devez télécharger le *fichier de configuration KPSN* sur le Serveur d'administration de Kaspersky Security Center pour l'intégration avec Kaspersky Managed Detection and Response. Ce fichier contient les paramètres nécessaires à l'envoi de télémétrie. Le fichier de configuration KPSN est un fichier avec l'extension .pkcs7 et se trouve dans l'archive ZIP du fichier de configuration MDR. Pour plus d'informations, consultez l'aide de Kaspersky Managed Detection and Response.

Vous pouvez télécharger le fichier de configuration KPSN dans Web Console ou dans la Console d'administration.

En chargeant le fichier de configuration KPSN, vous acceptez de transférer automatiquement les données de l'appareil sur lequel Kaspersky Endpoint Security est installé à Kaspersky à des fins de traitement. Ne chargez pas le fichier de configuration si vous n'acceptez pas le traitement des données transférées. Pour une description détaillée des données transmises, consultez la documentation de Kaspersky Managed Detection and Response.

Comment télécharger le fichier de configuration KPSN dans Web Console

1. Dans la fenêtre principale de Web Console, ouvrez la fenêtre des propriétés du Serveur d'administration.
2. Dans la liste de gauche, sélectionnez la section **Configuration du serveur proxy KSN**.

3. Activer la fonction **Activer le serveur proxy KSN sur le Serveur d'administration** pour activer le service du serveur proxy KSN.

4. Activez le bouton bascule **Utiliser Kaspersky Private Security Network**.

5. Dans la fenêtre qui s'ouvre pour vous avertir des particularités de l'utilisation du serveur proxy KSN sur des points de distribution sur lesquels est installée une ancienne version de l'Agent d'administration, cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **Fichier avec les paramètres du serveur proxy KSN**.

7. Sélectionnez le fichier de configuration KSN (fichier avec l'extension .pkcs7) et cliquez sur le bouton **Ouvrir**.

8. Acceptez les Conditions du KPSN et cliquez sur le bouton **Enregistrer**.

Comment télécharger le fichier de configuration KPSN dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration, ouvrez la fenêtre des propriétés du Serveur d'administration.

2. Sélectionnez la section **Serveur proxy KSN → Paramètres du serveur proxy KSN**.

3. Cochez la case **Utiliser le Serveur d'administration comme serveur proxy** pour activer le service du serveur proxy KSN.

4. Cochez la case **Configurer KPSN**.

5. Dans la fenêtre qui s'ouvre pour vous avertir des particularités de l'utilisation du serveur proxy KSN sur des points de distribution sur lesquels est installée une ancienne version de l'Agent d'administration, cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **Fichier avec les paramètres du serveur proxy KSN**.

7. Sélectionnez le fichier de configuration KSN (fichier avec l'extension .pkcs7) et cliquez sur le bouton **Ouvrir**.

8. Acceptez les Conditions du KPSN et cliquez sur le bouton **Appliquer**.

Comment télécharger le fichier de configuration KPSN via la ligne de commande

Exécutez la commande :

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

Comment configurer l'intégration MDR

Avant de configurer l'intégration de Kaspersky Managed Detection and Response :

- Autorisez la connexion sur les ports 443 et 1443.
- Autorisez les connexions aux adresses suivantes :
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

  La liste des adresses est susceptible d'être modifiée. Pour obtenir l'adresse exacte, vous pouvez contacter le Support technique.
- Assurez-vous que les éléments suivants sont activés et fonctionnent :
  - Kaspersky Security Network en mode étendu :
  - Détection comportementale.

    Pour vous assurer que la télémétrie est complète, vous pouvez également activer les modules suivants : Protection contre les menaces Internet, Protection contre les menaces réseau, Protection contre les fichiers malicieux et Protection contre les menaces par emails.

Étapes essentielles de la configuration

1. **Activez le module MDR de l'une des manières suivantes**

   - À l'aide d'une clé de licence.

     Ajoutez la clé de licence MDR à l'application si vous avez acheté une licence distincte pour utiliser cette fonctionnalité.

     Si vous utilisez Kaspersky Endpoint Security sous une licence qui inclut Kaspersky Managed Detection and Response, aucune action n'est requise.

     Si Kaspersky Endpoint Security est utilisé en mode Light Agent, la clé de licence MDR est ajoutée à la SVM.

   - À l'aide d'un fichier BLOB MDR.

     Dans la console MDR, téléchargez le fichier de configuration MDR. Ce fichier est une archive ZIP contenant un fichier BLOB MDR et un fichier de configuration KPSN.

     Chargez ensuite le fichier BLOB dans la Web Console, dans la Console d'administration ou via la ligne de commande.

   La version de l'application Kaspersky Endpoint Security détermine la méthode d'activation du module MDR ainsi que la nécessité ou non d'utiliser le fichier de configuration KPSN. Pour plus d'informations, consultez l'aide de Kaspersky Managed Detection and Response.

Si les Serveurs d'administration de Kaspersky Security Center sont organisés en hiérarchie et que le serveur secondaire ne dispose d'aucun accès direct à Internet, Kaspersky Managed Detection and Response ne peut pas fonctionner, même si le Serveur d'administration primaire dispose d'un accès à Internet.

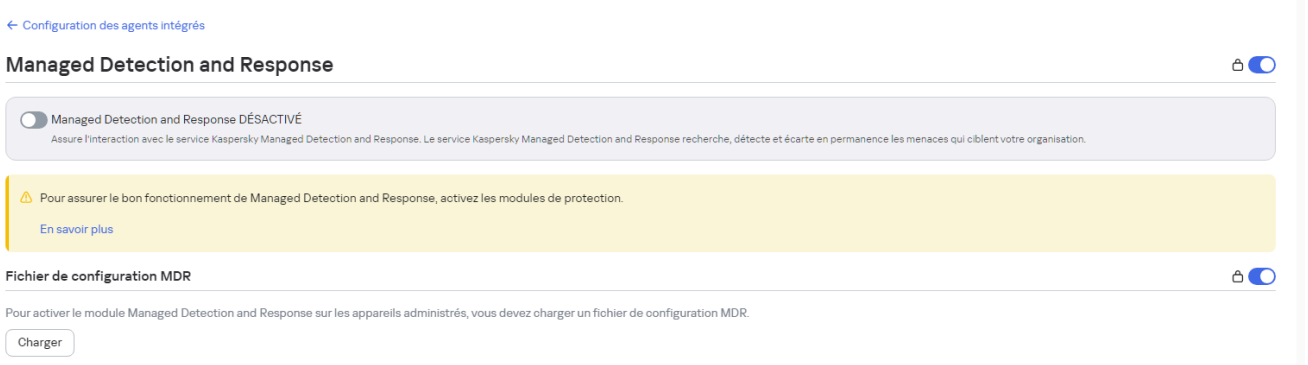
2 Chargez le fichier de configuration KPSN

Si votre organisation compte plusieurs locataires ou si vous avez activé le module MDR à l'aide d'un fichier BLOB MDR, chargez le fichier KPSN sur le Serveur d'administration de Kaspersky Security Center. Ce fichier contient les paramètres nécessaires à l'envoi de la télémétrie ; vous le trouverez dans l'archive ZIP qui contient le fichier de configuration MDR.

3 Configurez les paramètres d'intégration avec Kaspersky Managed Detection and Response

Comment activer l'intégration avec Kaspersky Managed Detection and Response dans la Web Console

1. Dans la fenêtre principale de la Web Console, sélectionnez la section **Gestion des ressources → Stratégies**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security requise.
3. Dans la fenêtre des propriétés de la stratégie qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Dans la section **Configuration des agents intégrés**, sélectionnez **Managed Detection and Response**, puis, dans la partie droite de l'écran, configurez les paramètres suivants :
   - Réglez le commutateur sur **Managed Detection and Response ACTIVÉ**.
   - Si vous disposez de locataires ou si vous avez activé le module MDR à l'aide d'un fichier BLOB MDR, cliquez sur le bouton **Charger** pour ajouter un fichier BLOB MDR.
5. Enregistrez les paramètres.



Managed Detection and Response

Comment activer l'intégration avec Kaspersky Managed Detection and Response via la ligne de commande

1. Pour activer le module MDR, exécutez la commande suivante :

```
kesl-control --set-app-settings UseMDR=Yes
```

2. Pour ajouter un fichier BLOB, exécutez la commande suivante :

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4. **Configurez la stratégie KSN**

Comment gérer les paramètres KSN dans la Web Console

1. Dans la stratégie de Kaspersky Endpoint Security, sous l'onglet **Paramètres de l'application**, accédez à la section **Paramètres généraux**.

2. Sélectionnez **Kaspersky Security Network**, puis, dans la partie droite de l'écran, indiquez les paramètres suivants :

   a. Réglez le commutateur sur **Utilisation de Kaspersky Security Network (KSN) ACTIVÉE**.

   b. Dans la sous-section **Paramètres de KSN**, cochez la case **Utiliser le mode étendu de KSN**.

   c. Dans la sous-section **Serveur proxy KSN**, cochez les cases suivantes :

   - **Utiliser le Serveur d'administration comme serveur proxy KSN**
   - **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**

   La télémétrie sera collectée depuis le Serveur d'administration ou depuis l'appareil, selon la disponibilité des options configurées.

3. Enregistrez les paramètres.

Comment configurer les paramètres KSN via la ligne de commande

Pour activer KSN en mode étendu, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **Activer KSN**

Comment activer KSN dans la Web Console

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

2. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez la section **Proxy KSN**.

3. Réglez le commutateur sur **Activer le proxy KSN sur le Serveur d'administration Activé**.

4. Activez le commutateur correspondant à la solution d'infrastructure KSN que vous utilisez :

   - **Utiliser Kaspersky Security Network Activé**.
   - **Utiliser Kaspersky Private Security Network Activé**, puis chargez le fichier de configuration KPSN.

5. Enregistrez les paramètres.

6. **Assurez-vous que la connexion à Kaspersky Managed Detection and Response a été établie correctement**

   Vérifiez l'état de Kaspersky Managed Detection and Response de la manière qui vous convient.

Comment vérifier que l'intégration MDR est activée

Vous pouvez vérifier la santé du module Kaspersky Managed Detection and Response de l'une des manières suivantes :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

  L'intégration de Kaspersky Managed Detection and Response s'affiche avec l'état **Disponible et en cours d'exécution**.

- Dans la Console MDR, accédez à la section **Actifs**. Les appareils s'affichent avec l'état **OK** (vert).

Si le module est désactivé :

1. Mettez à jour les bases antivirus de l'application.
2. Assurez-vous que Kaspersky Security Network est activé et fonctionne en mode avancé.
3. Vérifiez les clés de licence pour Kaspersky Endpoint Security et MDR.
4. Assurez-vous que le fichier BLOB a été ajouté à la stratégie.
5. Vérifiez que les modules dont MDR a besoin sont en état de fonctionnement.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux prend en charge la solution Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* est une solution de gestion de la sécurité des informations et des événements (SIEM) pour l'infrastructure informatique des organisations. KUMA permet de détecter, d'analyser et d'atténuer les menaces à la sécurité avant qu'elles ne causent des dommages.

Pour plus d'informations sur la solution, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les informations relatives aux événements survenus sur l'ordinateur (télémétrie) sont envoyées au serveur Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Le module n'est pas disponible pour les appareils équipés d'un processeur Elbrus.

Comment configurer l'intégration KUMA

Avant de configurer l'intégration avec Kaspersky Unified Monitoring and Analysis Platform :

- Autorisez les connexions aux ports 443 et 1443 ou aux ports configurés côté collecteur KUMA.
- Ajoutez la clé de licence KUMA à l'application si vous avez acheté une licence distincte pour utiliser cette fonctionnalité.

  Si vous utilisez Kaspersky Endpoint Security sous une licence qui inclut Kaspersky Unified Monitoring and Analysis Platform, aucune action n'est requise.

  Si l'application est utilisée en mode Light Agent, la clé de licence KUMA est ajoutée à la SVM.

Étapes essentielles de la configuration

1. **Dans KUMA, configurez un collecteur et un normalisateur.**

   Si vous souhaitez utiliser un certificat client, lors de la configuration du collecteur dans l'onglet **Transport**, sélectionnez le type de connecteur tcp. Ensuite, dans l'onglet **Paramètres avancés**, dans la **liste déroulante Mode TLS**, sélectionnez **PFX personnalisé avec authentification du client**.

2. **Copier l'adresse du collecteur auquel se connecter**

   Dans la section **Ressources** → **Services actifs**, dans le tableau des services, copiez et enregistrez par tout moyen pratique les valeurs des colonnes **FQDN / Adresse IP** et **Port**.

   Si vous utilisez TLS pour la connexion, indiquez uniquement le nom de domaine complet (FQDN). La valeur du paramètre est sensible à la casse.

3. **Obtenir et traiter les certificats émis par le serveur KUMA**

   L'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge pour les connexions UDP au serveur KUMA.

   Un serveur proxy est utilisé pour se connecter au serveur KUMA si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application Kaspersky Endpoint Security.

   Obtenez le Certificat du serveur (certificat de l'autorité de certification des microservices), voir Téléchargement des certificats d'autorité de certification. Pour traiter le certificat, convertissez-le au format DER ou PEM en suivant les étapes de l'article Conversion d'un certificat PFX au format PEM.

Pour une protection supplémentaire, vous pouvez également utiliser un certificat client obtenu lors de la configuration du collecteur, voir l'étape 1.

4. **Configurer les paramètres de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform**

Comment configurer l'intégration KUMA dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Intégration KUMA**.
5. Activez le commutateur **Intégration KUMA ACTIVÉE**.
6. Ajoutez des serveurs KUMA :
   a. Cliquez sur **Ajouter**.

      Cette action ouvre le formulaire dans lequel vous pouvez ajouter des serveurs KUMA.
   b. Sélectionnez le protocole de connexion au serveur KUMA : **HTTP/HTTPS**, **TCP** ou **UDP**.

      Le protocole de connexion au collecteur dans Kaspersky Endpoint Security doit correspondre au type de connecteur dans KUMA : **http**, **tcp** ou **udp**.

      Si vous sélectionnez le protocole **HTTP/HTTPS**, l'application utilise par défaut le protocole HTTPS pour la connexion aux serveurs KUMA. Pour utiliser le protocole HTTP, vous devez indiquer ce protocole manuellement dans l'adresse du serveur (par exemple, `http://server.com`).
   c. Indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur (le port 443 est spécifié par défaut).

      Vous pouvez consulter l'adresse du serveur dans les propriétés du connecteur de la console KUMA. Pour plus d'informations sur les connecteurs KUMA, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.
   d. Cliquez sur **OK**.

   Kaspersky Endpoint Security se connecte au premier serveur KUMA de la liste. En cas d'échec de la connexion, Kaspersky Endpoint Security se connecte au deuxième serveur KUMA de la liste et ainsi de suite.
7. Si nécessaire, configurez le paramètre **Durée d'attente maximale pour l'envoi des événements (sec)** dans le groupe **Paramètres de connexion au serveur**. Lorsque le délai spécifié est écoulé, Kaspersky Endpoint Security tente de se connecter au même collecteur ou se connecte au collecteur suivant dans la liste s'il y a plusieurs collecteurs. Le paramètre par défaut est de 30 secondes.
8. Enregistrez vos modifications.

Comment configurer l'intégration KUMA en ligne de commande

1. Pour ajouter un serveur KUMA, exécutez la commande suivante :

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. Pour ajouter un certificat de serveur KUMA, exécutez la commande suivante :

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. Pour configurer les paramètres d'intégration, exécutez la commande suivante :

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

Les paramètres et leurs valeurs possibles sont répertoriés dans le tableau ci-dessous.

4. Pour ajouter un certificat client pour la connexion au serveur de réponse, exécutez la commande suivante :

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. Pour activer l'intégration avec EDR (KATA), exécutez la commande suivante :

```
kesl-control --start-task 33
```

Paramètres de la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform

Paramètre	Description	Valeur
`UseTls`	Activation ou désactivation de l'analyse du certificat du serveur pour sécuriser davantage la connexion au serveur KUMA.	`Yes` : utiliser le certificat pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser le certificat pour sécuriser la connexion au serveur KUMA.
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Si l'analyse du certificat client est activée du côté serveur KUMA, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KUMA en secondes.	Valeur par défaut : `5`.
La section **[Servers.item_#]** contient les paramètres du serveur KUMA.		
`ServerAddress`	Adresse du serveur KUMA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Si vous définissez `UseTls=Yes`, vous devez fournir le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat de votre licence KUMA.	Valeur par défaut : `127.0.0.1`.
`ServerPort`	Port de connexion au serveur KUMA.	Valeur par défaut : `443`.

Paramètre	Description	Valeur
`ServerProtocol`	Protocole pour se connecter au serveur KUMA.	`tcp` (valeur par défaut) : utiliser le protocole TCP pour la connexion au serveur KUMA. `HTTPWithCompression` : utiliser le protocole HTTP avec compression des événements pour se connecter au serveur KUMA. `udp` : utiliser le protocole UPD pour la connexion au serveur KUMA. Lorsque le protocole UDP est sélectionné, l'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge (les valeurs des paramètres `UseTls`, `UseClientCertificate` et `ConnectionTimeout` sont ignorées), et il n'y a aucun événement concernant la connexion au serveur KUMA.
La section **[KumaTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur KUMA.		
`EventTransferTimeMax`	Délai maximum en secondes pour l'envoi des événements au serveur KUMA.	Valeur par défaut : `30`.

5. **Assurez-vous que la connexion à Kaspersky Unified Monitoring and Analysis Platform a été établie avec succès**

   Vérifiez l'état de KUMA de la manière qui vous convient.

Comment vérifier que l'Intégration KUMA est opérationnelle

Vous pouvez tester le module KUMA des manières suivantes :

- Depuis la ligne de commande, à l'aide de la commande suivante :

  ```
  kesl-control --app-info
  ```

  L'intégration avec KUMA s'affiche avec l'état **Disponible et en cours d'exécution**.

- Dans la Web Console (console OSMP) :

  Accédez à la section **Recherche de menaces** : les événements de télémétrie dont l'état est « La connexion à KUMA a été établie » pour l'appareil concerné s'affichent dans la liste des événements.

- Dans Kaspersky Unified Monitoring and Analysis Platform :

  Dans le menu principal de la console KUMA, accédez à la section **Événements** : les événements de télémétrie de Kaspersky Endpoint Security s'affichent dans la liste.

Protection des environnements virtuels

Kaspersky Endpoint Security prend en charge le mode Light Agent pour fonctionner dans le cadre de Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* est une solution intégrée qui offre une protection complète pour les machines virtuelles contre divers types de menaces informatiques, de réseaux et d'attaques de phishing. Pour utiliser cette solution, il convient d'installer l'application en mode Light Agent.

Lorsque vous démarrez le Light Agent, il établit et maintient une connexion avec la machine virtuelle SVM (Secure Virtual Machine). Un Serveur de protection est déployé sur la SVM. Le *Serveur de protection* est le module de la solution Kaspersky Security for Virtualization Light Agent qui analyse les fichiers à la recherche de virus et autres programmes malveillants, met à jour les bases antivirus et gère les clés de licence. Le Light Agent envoie à la SVM les fichiers ou les fragments de fichiers qui doivent être analysés. Les résultats de l'analyse sont disponibles pour toutes les machines virtuelles sur lesquelles le Light Agent est installé (la technologie SharedCache). Cette technologie augmente l'efficacité de la solution et accélère la réaction aux menaces.

L'infrastructure de l'organisation peut contenir de nombreuses machines virtuelles sur lesquelles le Light Agent est installé, ainsi que de nombreuses SVM. Le Serveur d'intégration gère l'interaction entre les machines virtuelles et les SVM. Le *Serveur d'intégration* est un module de la solution Kaspersky Security for Virtualization Light Agent qui génère la liste des SVM disponibles et transfère ces données aux Light Agents, participe à la découverte des SVM par les Light Agents, protège la connexion entre les Light Agents et les SVM et assure d'autres fonctions.

À propos de la connexion Light Agent à la SVM

1. **Obtention d'une liste des SVM disponibles**

   Le Light Agent obtient la liste des SVM disponibles.

2. **Sélection du Serveur de protection (SVM) optimal**

   Le Light Agent détermine un Serveur de protection (SVM) disponible optimal pour la connexion en fonction de l'algorithme de sélection de la SVM.

3. **Vérification des paramètres de connexion supplémentaires**

   Le Light Agent vérifie les paramètres supplémentaires de connexion à la SVM : tags, état de protection de la connexion et fonctionnalités de l'application couvertes par la licence.

4. **À propos de la connexion Light Agent à la SVM**

   Le Light Agent établit et maintient une connexion avec la SVM sélectionnée.

Comment configurer la découverte des SVM

Pour le Light Agent, vous pouvez choisir une des méthodes de détection des SVM :

- À l'aide du Serveur d'intégration (VIIS).

  Le *Serveur d'intégration* est le module de la solution qui permet à Kaspersky Security for Virtualization Light Agent d'interagir avec l'infrastructure virtuelle et génère une liste des SVM disponibles pour la connexion. Le Light Agent établit une connexion avec le Serveur d'intégration et obtient la liste des adresses des SVM.

  Le Serveur d'intégration est particulièrement utile dans les grandes infrastructures virtuelles, car il équilibre automatiquement la charge entre les SVM, obtient des informations sur les SVM disponibles, analyse ces informations et fournit aux Light Agents une liste des Serveurs de protection (SVM) optimaux pour la connexion.

  Pour que le Light Agent puisse obtenir une liste des SVM, il suffit d'entrer l'adresse du Serveur d'intégration.

- Utilisation d'un cluster à haute disponibilité de Serveurs d'intégration.

Le déploiement d'un cluster à haute disponibilité de Serveurs d'intégration est disponible dans Kaspersky Security for Virtualization Light Agent 6.4. Un cluster à haute disponibilité de Serveurs d'intégration assure une protection ininterrompue de l'environnement virtuel grâce au basculement des SVM et des Light Agents vers un Serveur d'intégration de sauvegarde en cas de défaillance du Serveur d'intégration primaire. Un module spécial du cluster, l'*équilibreur de charge*, assure le basculement des serveurs. Pour en savoir plus sur le cluster à haute disponibilité de Serveurs d'intégration, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Pour que Light Agent obtienne la liste des SVM, vous devez saisir l'adresse de l'appareil sur lequel l'équilibreur de charge est installé.

- À l'aide de la liste d'adresses de SVM.

  Si vous devez spécifier des SVM particulières auxquelles vous souhaitez que le Light Agent se connecte, vous pouvez préparer une liste manuellement.

  Il convient de lister les adresses des SVM disponibles auxquelles le Light Agent peut se connecter.

Comment configurer la détection des SVM par le Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Mode Light Agent** → **Paramètres de détection des SVM**.
5. Sélectionnez une méthode de détection des SVM.
   - **Utiliser le Serveur d'intégration**. Saisissez les paramètres de connexion au Serveur d'intégration en fonction de votre infrastructure :
     - **Serveur d'intégration unique**. Saisissez les paramètres de connexion au Serveur d'intégration : adresse IPv4 ou nom de domaine complet (FQDN) de l'appareil.
     - **Cluster à haute disponibilité de Serveurs d'intégration**. Saisissez l'adresse IP et le port de l'équilibreur de charge qui fait partie du cluster.
   - **Utiliser la liste d'adresses des SVM définie manuellement**. Créez une liste des SVM auxquelles le Light Agent peut se connecter. Indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Chaque élément de la liste doit être placé sur une nouvelle ligne ou séparé de l'élément précédent par un point-virgule (`;`).

     La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans le texte.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Pour afficher les informations sur la connexion du Light Agent au Serveur d'intégration via la ligne de commande :

1. Assurez-vous que l'application est installée en mode Light Agent :

   ```
   kesl-control -V --ksvla-info
   ```

   Le module doit avoir l'état **Activé**.

2. Affichez les informations sur la connexion du Light Agent au Serveur d'intégration :

   ```
   kesl-control -V --viis-info
   ```

La commande affiche les informations suivantes sur la console :

- Adresse et port du Serveur d'intégration auquel le Light Agent se connecte.
- Statut de connexion au Serveur d'intégration.
- Date et heure de la dernière connexion du Light Agent avec le Serveur d'intégration.

Comment consulter les informations sur la connexion du Light Agent au Serveur d'intégration via la ligne de commande

1. Assurez-vous que l'application est installée en mode Light Agent :

   ```
   kesl-control -V --ksvla-info
   ```

   Le module doit avoir l'état **Activé**.

2. Affichez les informations sur la connexion du Light Agent au Serveur d'intégration :

   ```
   kesl-control -V --svm-info
   ```

La commande affiche les informations suivantes sur la console :

- L'adresse de la SVM à laquelle le Light Agent est connecté, et l'emplacement de la SVM dans l'infrastructure virtuelle par rapport au Light Agent : local ou non local.
- Méthode de recherche des SVM utilisée par le Light Agent : à l'aide d'un Serveur d'intégration ou d'une liste personnalisée d'adresses de la SVM spécifiées manuellement.
- Liste d'adresses SVM, si la liste d'adresses SVM est sélectionnée comme mode de détection SVM.
- Tag pour connecter le Light Agent à la SVM.
- Algorithme de sélection des SVM : standard ou avancé. Si l'algorithme de sélection SVM avancé est utilisé, le type d'emplacement de la SVM dans l'infrastructure virtuelle est également affiché.
- Disponibilité d'une protection de connexion entre le Light Agent et le Serveur de Protection.

Comment le Light Agent sélectionne les SVM

L'infrastructure de l'organisation peut avoir plusieurs SVM déployées auxquelles les Light Agents peuvent se connecter. Pour équilibrer la charge sur le réseau et les ressources de l'infrastructure virtuelle, vous devez répartir les Light Agents entre les SVM.

Algorithmes de sélection des SVM

Les Light Agents peuvent utiliser les algorithmes de sélection des SVM suivants pour la connexion : l'algorithme standard (par défaut) et l'algorithme étendu.

Algorithmes de sélection des SVM

Algorithme standard	Algorithme étendu
Si cet algorithme est utilisé, après l'installation et le démarrage, le Light Agent sur la machine virtuelle choisit de se connecter à la SVM qui est *locale* par rapport au Light Agent. Si aucune SVM locale adaptée à la connexion n'est trouvée, le Light Agent sélectionne une SVM à laquelle est connecté le plus petit nombre de Light Agents, quelle que soit la position de la SVM dans l'infrastructure virtuelle. Le caractère local de la SVM par rapport au Light Agent n'est pas déterminé si le mode de protection des grandes infrastructures est activé pour le Serveur de protection sur cette SVM. Dans ce cas, il est recommandé d'utiliser l'algorithme étendu de sélection des SVM et de sélectionner le Serveur d'intégration comme méthode de détection des SVM. Le fait qu'une SVM soit considérée comme locale pour un Light Agent dépend du type d'infrastructure virtuelle.	Si cet algorithme est appliqué, vous pouvez spécifier les paramètres suivants de sélection des SVM : • prendre en compte ou ignorer l'emplacement de la SVM dans l'infrastructure lors de la sélection d'une SVM pour la connexion ; • si l'emplacement de la SVM est pris en compte, la méthode pour déterminer la localité de la SVM par rapport à l'Agent Light Si les Light Agents ignorent l'emplacement de la SVM dans l'infrastructure, alors les Light Agents pourront se connecter à n'importe quelle SVM disponible pour la connexion. Si les Light Agents doivent prendre en compte l'emplacement de la SVM dans l'infrastructure, vous devez sélectionner le type d'emplacement de la SVM qui sera pris en compte pour déterminer la localité de la SVM par rapport au Light Agent. La question de savoir si une SVM est considérée comme locale pour un Light Agent dépend du type d'infrastructure virtuelle. Si les Light Agents prennent en compte l'emplacement de la SVM dans l'infrastructure lors de la sélection d'une SVM pour la connexion, alors les Light Agents ne peuvent se connecter qu'à la SVM locale. Par exemple, si vous désignez un cluster hyperviseur en tant que type d'emplacement des SVM, alors toutes les SVM déployées sur ce cluster hyperviseur seront considérés comme locales pour le Light Agent et le Light Agent pourra se connecter à une seule de ces SVM. En l'absence de SVM disponibles pour une connexion dans le cluster dans lequel fonctionne le Light Agent, le Light Agent ne se connecte pas à la SVM. Lors de la sélection des SVM, les Light Agents tiennent aussi compte du nombre de Light Agents connectés pour garantir une répartition équitable des Light Agents entre les SVM disponibles pour la connexion. Si un algorithme étendu de sélection des SVM est utilisé pour un Light Agent et que la liste d'adresses des SVM est sélectionnée comme méthode de détection des SVM et que le mode de protection des grandes infrastructures est activé sur la SVM, la connexion du Light Agent à cette SVM n'est possible que si le Light Agent ignore l'emplacement de la SVM.

Algorithme standard	Algorithme étendu
Basis Dynamix Enterprise	
Dans une infrastructure virtuelle basée sur Basis Dynamix Enterprise, toute SVM déployée sur le même nœud que la machine virtuelle sur laquelle Light Agent est installé est considérée comme une SVM locale pour Light Agent.	Dans une infrastructure virtuelle basée sur Basis Dynamix Enterprise, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM est déployée sur le même nœud que celui où se trouve la machine virtuelle dotée de Light Agent. • Une SVM est déployée dans la même zone que celui où se trouve la machine virtuelle dotée de Light Agent. • Une SVM est déployée dans le même centre de données que la machine virtuelle dotée de Light Agent.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer et Basis Dynamix Standard	
Dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, toute SVM déployée sur le même hyperviseur que la machine virtuelle sur laquelle Light Agent est installé est considérée comme une SVM locale pour Light Agent.	Dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM est déployée sur le même hyperviseur que la machine virtuelle dotée de Light Agent. • Une SVM est déployée sur le même cluster hyperviseur que la machine virtuelle dotée de Light Agent.Agent. • Une SVM est déployée dans le même centre de données que la machine virtuelle dotée de Light Agent.
OpenStack et VK Private Cloud SVM	
Dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud, vous pouvez spécifier comment la localité de la SVM par rapport au Light Agent est déterminée à l'aide du paramètre `StandardAlgorithmSvmLocality` dans la section `HypervisorSpecificSettings:Openstack` dans le fichier de configuration appsettings.json du Serveur d'intégration. Selon la version du Serveur d'intégration, le fichier se trouve dans le chemin suivant : • /var/opt/kaspersky/viis/common/ : fichier du Serveur d'intégration sous Linux. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ : fichier du Serveur d'intégration sous Windows. Le paramètre `StandardAlgorithmSvmLocality` peut prendre les valeurs suivantes : • `ServerGroup` : si cette valeur est définie, on considère comme SVM locale pour Light Agent toute SVM qui se trouve dans le même groupe de serveurs que la machine virtuelle dotée de Light Agent. Cette valeur est utilisée par défaut. • `Project` : si cette valeur est définie, on considère comme SVM locale pour Light Agent la SVM déployée dans le cadre du même projet OpenStack que celui de la machine virtuelle avec Light Agent. • `AvailabilityZone` : si cette valeur est définie, on considère comme SVM locale pour Light Agent la SVM qui se trouve dans la même zone de disponibilité que la machine virtuelle dotée de Light Agent.	Dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM se trouve dans le même groupe de serveurs que la machine virtuelle dotée du Light Agent. • Une SVM est déployée dans le même projet OpenStack que la machine virtuelle dotée de Light Agent. • Une SVM se trouve dans la même zone de disponibilité que la machine virtuelle dotée de Light Agent.

En plus des algorithmes de connexion à la SVM, vous pouvez réguler la connexion des Light Agents aux SVM à l'aide des tags.

Comment configurer l'algorithme de sélection des SVM pour le Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Mode Light Agent** → **Algorithme de sélection des SVM**.

5. Sélectionnez l'algorithme :

- **Utiliser l'algorithme standard de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le même hyperviseur.

- **Utiliser l'algorithme étendu de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le type de chemin d'accès à la SVM sélectionné (par défaut, **Hyperviseur**).

6. Si nécessaire, sélectionnez les chemin d'accès à la SVM pour l'algorithme étendu de sélection de la SVM :

- **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - La SVM se trouve dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve sur le même nœud que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  S'il n'y a aucune SVM disponible pour la connexion sur le même hyperviseur ou dans le même groupe de serveurs où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Cluster**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM sont déployées dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans la même zone que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Bais Dynamix Enterprise).

  S'il n'y a aucune SVM disponible à laquelle se connecter dans le même cluster d'hyperviseur ou dans le même projet OpenStack où se trouve la machine virtuelle Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Centre de données**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM se trouvent dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  En l'absence de SVM disponible pour la connexion dans le même centre de données ou la même zone de disponibilité que la machine virtuelle avec le Light Agent, ce dernier ne se connecte pas à la SVM.

- **Ignorer**. Le Light Agent ignore le chemin d'accès à la SVM pour se connecter au Serveur de protection. Le Light Agent prend en compte d'autres critères, comme les tags, le nombre de Light Agents connectés à une SVM, etc.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment équilibrer la connexion des Light Agents entre les SVM

Plusieurs Light Agents peuvent se connecter à une SVM. Pour équilibrer les connexions des Light Agents, vous pouvez spécifier une liste distincte de SVM. Si vous utilisez un Serveur d'intégration pour la découverte des SVM, vous pouvez utiliser les *tags* pour équilibrer les connexions du Light Agent aux SVM. Autrement dit, pour un Light Agent, vous pouvez désigner une liste de SVM auxquelles se connecter à l'aide d'un tag. Pour ce faire, il convient d'attribuer un tag au Light Agent et de spécifier ce tag dans les paramètres de la SVM. Pour en savoir plus sur la définition des tags dans les paramètres de la SVM, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Exemple : la solution Kaspersky Endpoint Detection and Response Optimum est déployée dans votre infrastructure pour les hôtes de machines virtuelles désignés. Dans ce cas, vous pouvez attribuer le tag `[EDROptimum]` au Light Agent pour le connecter aux SVM auxquelles la clé de licence EDR Optimum (module complémentaire EDR Optimum) a été ajoutée. Par conséquent, vous pouvez utiliser la fonctionnalité EDR Optimum sur la machine virtuelle avec le Light Agent. Lors de la connexion du Light Agent à une SVM sans clé de licence EDR Optimum, la fonctionnalité de Kaspersky Endpoint Detection and Response Optimum n'est pas disponible.

Comment attribuer un tag de connexion SVM à un Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Mode Light Agent** → **Tag de connexion à la SVM**.

5. Cochez la case **Utiliser le tag de connexion** et saisissez un tag de connexion à la SVM.

   En guise de tag, vous pouvez saisir un texte de 255 caractères maximum. Vous pouvez utiliser n'importe quel caractère à l'exception du caractère `;`.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Protection de la connexion entre le Light Agent et une SVM

Vous pouvez configurer le chiffrement de la connexion entre les Light Agents et le Serveur de protection. Pour ce faire, vous devez activer le chiffrement du canal de données entre le Light Agent et le Serveur de protection dans les paramètres du Serveur de protection sur la SVM ainsi que dans les paramètres du Light Agent.

Un Light Agent pour lequel la protection des connexions est activée peut se connecter uniquement aux SVM pour lesquelles le chiffrement du canal de données entre le Light Agent et le Serveur de protection est activé. Un Light Agent pour lequel la protection des connexions est désactivée peut se connecter uniquement aux SVM pour lesquelles le chiffrement du canal est désactivé ou pour lesquelles une connexion non sécurisée entre le Serveur de protection et le Light Agent est autorisée.

Pour en savoir plus sur la configuration de la protection des connexions sur le Serveur de protection, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

La protection de la connexion à l'aide du chiffrement peut réduire les performances de Kaspersky Security for Virtualization Light Agent.

Comment configurer la protection des connexions dans un Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Mode Light Agent** → **Protection de la connexion**.
5. Cochez la case **Chiffrer le canal de données entre le Light Agent et le Serveur de protection**.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment connaître l'état du Light Agent

Sur la ligne de commande, vous pouvez consulter les informations suivantes sur l'application utilisée en mode Light Agent :

- à propos des paramètres d'utilisation de l'application en mode Light Agent ;
- sur la connexion du Light Agent au Serveur d'intégration ;
- sur la connexion du Light Agent à la SVM.

Affichage des informations sur les paramètres d'utilisation de l'application en mode Light Agent

```
kesl-control [-V] --ksvla-info
```

La commande affiche les informations suivantes sur la console :

- Mode Light Agent pour protéger les environnements virtuels : Activé ou Désactivé.

  Si le mode Light Agent est activé, l'application est utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent.

- Mode de protection de l'infrastructure VDI : Activé ou Désactivé.

  Le mode de protection de l'infrastructure VDI vous permet d'optimiser le fonctionnement de l'application Kaspersky Endpoint Security sur les machines virtuelles temporaires. Lorsque le mode de protection VDI est activé, les mises à jour nécessitant un redémarrage de la machine virtuelle protégée ne sont pas installées sur les machines virtuelles temporaires. Lors de la réception de mises à jour nécessitant un redémarrage, le Light Agent installé sur une machine virtuelle temporaire envoie un message à Kaspersky Security Center concernant la nécessité de mettre à jour le modèle des machines virtuelles protégées.

- Type de machine virtuelle : persistant ou non persistant.

- Rôle de la machine virtuelle : Serveur ou Poste de travail.

- Identifiant de la machine virtuelle – UUID.

Affichage des informations concernant la connexion du Light Agent au Serveur d'intégration

```
kesl-control [-V] --viis-info
```

La commande affiche les informations suivantes sur la console :

- Adresse et port du Serveur d'intégration auquel le Light Agent se connecte.

- Statut de connexion au Serveur d'intégration.

- Date et heure de la dernière connexion du Light Agent avec le Serveur d'intégration.

Si votre infrastructure déploie un cluster tolérant aux pannes des Serveurs d'intégration basé sur Linux, l'adresse et le port du répartiteur de charge sont affichés. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Affichage des informations concernant la connexion du Light Agent à une SVM

```
kesl-control [-V] --svm-info
```

La commande affiche les informations suivantes sur la console :

- L'adresse de la SVM à laquelle le Light Agent est connecté, et l'emplacement de la SVM dans l'infrastructure virtuelle par rapport au Light Agent : local ou non local.
- Méthode de recherche des SVM utilisée par le Light Agent : à l'aide d'un Serveur d'intégration ou d'une liste personnalisée d'adresses de la SVM spécifiées manuellement.
- Liste d'adresses SVM, si la liste d'adresses SVM est sélectionnée comme mode de détection SVM.
- Tag pour connecter le Light Agent à la SVM.
- Algorithme de sélection des SVM : standard ou avancé. Si l'algorithme de sélection SVM avancé est utilisé, le type d'emplacement de la SVM dans l'infrastructure virtuelle est également affiché.
- Disponibilité d'une protection de connexion entre le Light Agent et le Serveur de Protection.

Pour plus d'informations sur les paramètres de connexion des Light Agents au Serveur d'intégration et à la SVM, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent.

Bonnes pratiques

Lors du déploiement de Kaspersky Endpoint Security for Linux, vous pouvez utiliser les recommandations décrites dans cette section pour configurer la protection de l'ordinateur et optimiser les performances. Pour en savoir plus sur les problèmes de performances informatiques, consultez la Base de connaissances du support technique.

Optimisation de l'utilisation des ressources par l'application

Lorsque l'application s'exécute avec les paramètres par défaut, les performances du système peuvent diminuer sur certains appareils en raison de l'utilisation partagée des ressources système par les applications appliquées et l'application Kaspersky Endpoint Security.

Scénario de configuration recommandé pour optimiser la consommation des ressources système par l'application :

1. **Répartition des appareils en groupes d'administration en fonction du rôle des appareils dans l'infrastructure**

   Effectuez un inventaire des appareils selon les fonctions qu'ils exécutent et placez-les dans différents groupes d'administration selon ces fonctions. Par exemple, placez les serveurs Web dans un groupe d'administration, placez les serveurs de base de données dans un autre groupe d'administration, placez les postes de travail des utilisateurs dans un troisième groupe d'administration, etc.

2. **Configuration de l'application pour les rôles de serveur typiques**

   Configurez l'application sur les appareils en fonction de leur rôle dans l'infrastructure, conformément aux recommandations.

3. **Analyse des performances sur les appareils pilotes**

   Sélectionnez un ou deux appareils pilotes dans chaque groupe d'administration. Pour chaque appareil, analysez la manière dont l'application Kaspersky Endpoint Security utilise les ressources système et comment les performances des applications installées sur les appareils évoluent.

4. **Configuration des paramètres de l'application sur les appareils pilotes en fonction des résultats de l'analyse des performances**

   Si les performances des applications diminuent considérablement ou si la quantité de ressources système consommées par Kaspersky Endpoint Security est critique pour le fonctionnement du système d'exploitation et des applications, effectuez la configuration recommandée de la Protection contre les fichiers malicieux et les tâches d'analyse.

   Pour réduire l'impact des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Détection comportementale sur les performances de vos applications, optimisez les performances de ces modules.

5. **Configuration de l'application sur tous les appareils.**

   Si les étapes ci-dessus entraînent une amélioration des performances de votre appareil, veuillez effectuer une configuration similaire de l'application sur d'autres appareils du même type.

Analyse du fonctionnement de l'application sur l'appareil

Pour analyser les objets, l'application Kaspersky Endpoint Security utilise les ressources du processeur, les entrées et sorties du sous-système de disque et la mémoire vive.

Consulter les informations sur la consommation des ressources par l'application

```
top -bn1|grep kesl
```

Il faut exécuter la commande lors du chargement dans le système.

La commande renvoie la quantité de mémoire utilisée et le temps de processeur :

```
651 root       20      0 3014172 2.302g 154360 S 120.0 30.0    0:32.80 kesl
```

La colonne 6 affiche la quantité de mémoire résidente : 2.302g.

La colonne 9 reprend le pourcentage d'utilisation des cœurs du processeur – 120.0, où chaque cœur est utilisé à 100 %. Ainsi, 120 % signifie qu'un processeur est occupé à 100 % et le deuxième, à 20 %.

Pour obtenir des informations sur les performances de l'application, vous pouvez également configurer la collecte des métriques des ressources du système d'exploitation utilisées par l'application.

Si l'exécution de l'application Kaspersky Endpoint Security ralentit considérablement votre système, vous devez déterminer quels modules et tâches de l'application occupent des ressources système.

Pour ce faire, effectuez les expériences suivantes sur l'appareil :

1. **Analysez la consommation de ressources de la tâche Protection contre les fichiers malicieux (tâche de type OAS)**

   Par conséquent, vous serez en mesure de déterminer si les problèmes de performances sont liés à la tâche Protection contre les fichiers malicieux ou aux tâches d'analyse (tâches de types ODS et ContainerScan) et de mettre en œuvre les recommandations relatives aux tâches correspondantes.

   Comment analyser la consommation de ressources de la tâche Protection contre les fichiers malicieux

   1. Arrêtez toutes les tâches d'analyse et de surveillance.
   2. Assurez-vous que les tâches d'analyse à la demande (tâches de types ODS et ContainerScan) ne sont pas planifiées pour s'exécuter pendant l'analyse :
      a. Obtenez la liste de toutes les tâches de l'application :

      ```
      kesl-control --get-task-list
      ```

b. Obtenez les paramètres de planification de toutes les tâches de types ODS et ContainerScan :

```
kesl-control --get-schedule <task ID |name>
```

Si la commande renvoie `RuleType=Manual`, la tâche est uniquement exécutée manuellement.

c. Pour toutes les tâches qui ont une valeur `RuleType` différente de `Manual`, modifiez la planification :

```
kesl-control --set-schedule <task ID |name> RuleType=Manual
```

3. Activez la génération de fichiers de traçage de l'application avec un niveau de détail élevé :

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Si la tâche Protection contre les fichiers malicieux n'est pas en cours d'exécution, lancez-la :

```
kesl-control --start-task 1
```

5. Soumettez le système à une charge dans le même mode que celui qui a provoqué les problèmes de performances. Quelques heures suffisent.

6. Analysez les fichiers de traçage résultants. Par défaut, les fichiers de traçage sont enregistrés dans le répertoire /var/log/kaspersky/kesl.

> Quand elle est soumise à une charge, l'application enregistrer beaucoup d'information dans les fichiers de travail. Par défaut, le système conserver 10 fichiers de 500 Mo chacun. Pour cette raison, les informations les plus anciennes sont supprimées.

Si les problèmes de performances et de consommation de ressources persistent, il peut être nécessaire d'optimiser la Protection contre les fichiers malicieux.

Si les problèmes de performances et de consommation de ressources ne se produisent plus, ils sont probablement causés par des tâches d'analyse à la demande (tâches de types ODS et ContainerScan) ou par la tâche Détection comportementale. Vous devez optimiser les tâches d'analyse ou analyser les performances de la tâche Détection comportementale.

7. Désactivez la création de fichiers de traçage de l'application :

```
kesl-control --set-app-settings TraceLevel=None
```

2. **Analysez la consommation de ressources de la tâche Détection comportementale (tâche de type Behavior_Detection).**

Vous pouvez ainsi déterminer si les problèmes de performances sont liés à la tâche Détection comportementale ou aux tâches d'analyse (tâches de types ODS et ContainerScan), puis suivre les recommandations relatives aux tâches concernées.

Comment analyser la consommation de ressources de la tâche Détection comportementale

1. Arrêtez toutes les tâches d'analyse et de surveillance.
2. Assurez-vous que les tâches d'analyse à la demande (tâches de types ODS et ContainerScan) ne sont pas planifiées pour s'exécuter pendant l'analyse :
   a. Obtenez la liste de toutes les tâches de l'application :

   ```
   kesl-control --get-task-list
   ```

   b. Obtenez les paramètres de planification de toutes les tâches de types ODS et ContainerScan :

   ```
   kesl-control --get-schedule <task ID|name>
   ```

   Si la commande renvoie `RuleType=Manual`, la tâche est uniquement exécutée manuellement.

   c. Pour toutes les tâches qui ont une valeur `RuleType` différente de `Manual`, modifiez la planification :

   ```
   kesl-control --set-schedule <task ID|name> RuleType=Manual
   ```

3. Activez la génération de fichiers de traçage de l'application avec un niveau de détail élevé :

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Si la tâche Détection comportementale n'est pas en cours d'exécution, lancez-la :

   ```
   kesl-control --start-task 20
   ```

5. Soumettez le système à une charge dans le même mode que celui qui a provoqué les problèmes de performances. Quelques heures suffisent.
6. Analysez les fichiers de traçage résultants. Par défaut, les fichiers de traçage sont enregistrés dans le répertoire /var/log/kaspersky/kesl.

   Quand elle est soumise à une charge, l'application enregistrer beaucoup d'information dans les fichiers de travail. Par défaut, le système conserver 10 fichiers de 500 Mo chacun. Pour cette raison, les informations les plus anciennes sont supprimées.

   Si les problèmes de performances et de consommation de ressources persistent, il peut être nécessaire d'optimiser la Détection comportementale.

   Si les problèmes de performances et de consommation de ressources ne se produisent plus, les problèmes sont probablement causés par des tâches d'analyse à la demande (tâches de types ODS et ContainerScan). Il est nécessaire d'optimiser le travail de ces tâches.

7. Désactivez la création de fichiers de traçage de l'application :

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

3 Identifier les processus dont Kaspersky Endpoint Security détecte le lancement le plus souvent

Vous pouvez exclure de l'analyse les processus non dangereux lancés fréquemment afin d'optimiser les performances de la Détection comportementale.

Comment identifier les processus lancés le plus souvent

Exécutez la commande :

```
kesl-control --get-statistic --processes
```

Cette commande affiche la liste des processus dont Kaspersky Endpoint Security détecte le plus fréquemment le lancement, ainsi que le nombre de lancements de ces processus.

4 Identifier les chemins où les interceptions d'opérations sur les fichiers sont les plus fréquentes

Vous pouvez exclure des répertoires de l'interception des opérations sur les fichiers afin d'optimiser les performances de la Protection contre les fichiers malicieux et des tâches d'analyse.

Comment obtenir des informations sur l'interception des opérations sur les fichiers

Vous pouvez obtenir des informations sur l'interception des opérations sur les fichiers de l'une des manières suivantes :

- Obtenez des statistiques sur les fichiers que le module Protection contre les fichiers malicieux analyse le plus souvent :

  ```
  kesl-control --get-statistic --files
  ```

  La commande permet d'afficher des statistiques sur les opérations sur les fichiers interceptées au cours des dernières 24 heures.

- Utilisez les fichiers de traçage de l'application pour une analyse plus détaillée. En analysant les fichiers de traçage, vous pouvez obtenir une liste des fichiers interceptés par l'application et identifier les chemins où se produisent un grand nombre d'interceptions d'opérations de fichiers.

  Par défaut, les fichiers de traçage ne sont pas créés.

  Activer la création de fichiers de traçage

  ```
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  > L'activation du traçage peut avoir un impact négatif sur les performances globales du système. Il est recommandé de désactiver la création de fichiers de traçage lorsque le besoin d'enregistrer des traces disparaît.

  Désactiver la création de fichiers de traçage

  ```
  kesl-control --set-app-settings TraceLevel=None
  ```

- Obtenez la liste des fichiers interceptés :

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'|sort | uniq -c | sort -k1 -n -r
```

Si vous devez agréger les statistiques d'interception des opérations sur les fichiers dans les sous-répertoires jusqu'à une certaine profondeur à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X correspond à la profondeur d'imbrication. Par exemple :

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
```

5 Identifier les objets les plus fréquemment analysés

Si les actions effectuées lors des étapes précédentes ne suffisent pas, vous pouvez exclure de l'analyse les objets et fichiers non dangereux fréquemment analysés afin d'optimiser les performances de la Protection contre les fichiers malicieux et des tâches d'analyse.

Déterminez si les objets qui ont été analysé le plus souvent sont dangereux. Par exemple, les fichiers de base de données, les répertoires et les fichiers journaux peuvent être considérés comme sûrs s'ils sont écrits par un processus de confiance. En cas de difficultés, contactez le Support technique.

Comment identifier les objets les plus fréquemment analysés

1. Obtenez la liste des objets qui ont été analysés le plus souvent :

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

Le résultat est chargé dans l'utilitaire de visualisation de texte less, où les objets qui ont été analysés le plus souvent s'affichent en premier.

Si vous devez agréger les statistiques d'analyse des objets dans les sous-répertoires jusqu'à une certaine profondeur à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X correspond à la profondeur d'imbrication. Par exemple :

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c | sort -k1 -n -r|less
```

2. Si divers services enregistrent souvent des fichiers, ces fichiers seront à nouveau analysés dans la fille d'attente. Obtenez la liste des chemins qui ont été analysés le plus souvent dans la file d'attente :

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' | sort | uniq -c | sort -k1 -n -r
```

Les fichiers analysés le plus souvent apparaissent en début de liste.

Si vous devez agréger les statistiques d'analyse des objets dans les sous-répertoires jusqu'à une certaine profondeur à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X correspond à la profondeur d'imbrication. Par exemple :

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' | tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

Vous pouvez analyser les performances de l'application à l'aide de la ligne de commande. Si l'appareil est administré par une stratégie de Kaspersky Security Center, autorisez l'administration des tâches locales

pendant l'étude.

Recommandations pour la Protection contre les fichiers malicieux et les tâches d'analyse

Recommandations générales

Exclusions de l'analyse

Les exclusions de vérification aident à maintenir un équilibre entre la sécurité et les performances du système.

Nous vous recommandons d'exclure les éléments suivants de l'analyse :

- Les fichiers de données et les fichiers d'index des bases de données. Selon les experts antivirus de Kaspersky, ces fichiers ne présentent aucun risque de propagation des virus.
- Les objets non dangereux de la liste des objets les plus fréquemment analysés.

Les exclusions peuvent être configurées par chemin (y compris le type de montage), masque de fichier, type de menace et chemin d'accès au processus effectuant les opérations de fichier.

L'application ne vérifie pas les objets exclus de l'analyse, mais des retards minimes dans les opérations sur les fichiers sont présents, car l'application intercepte et bloque toujours les opérations sur les fichiers. Si vous devez éviter même des retards minimes, nous vous recommandons de configurer des exclusions de l'interception des opérations sur les fichiers.

Comment configurer les exclusions :

- Vous pouvez configurer des exclusions pour la Protection contre les fichiers malicieux dans une stratégie à l'aide de Web Console ou de la Console d'administration, ou localement sur l'appareil à l'aide de la ligne de commande.
- Vous pouvez configurer des exclusions pour les tâches d'analyse de type ODS et ContainerScan dans les paramètres des tâches dans Kaspersky Security Center ou localement sur l'appareil à l'aide de la ligne de commande.

  Les exclusions configurées pour une tâche d'analyse n'affectent pas les autres tâches d'analyse. Chaque tâche d'analyse nécessite que vous configuriez ses propres exclusions.

Exemples d'exclusions pour la Protection contre les fichiers malicieux configurées à l'aide de la ligne de commande

```
Exclure le répertoire /tmp/logs ainsi que tous les sous-répertoires et fichiers de manière récursive
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

```
Exclure un fichier spécifique ou des fichiers selon un masque dans le répertoire /tmp/logs
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

```
Exclure tous les fichiers avec l'extension .log dans le répertoire /tmp et ses sous-répertoires à l'aide d'un masque récursif
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Exclusions de l'interception des opérations sur les fichiers

Les fichiers exclus de l'analyse peuvent toujours être interceptés par l'application pendant la Protection contre les fichiers malicieux et les tâches d'analyse. L'application intercepte les événements d'opération de fichier et bloque les actions jusqu'à ce que les événements soient traités. Après analyse, l'application peut :

- enlever le blocage et laisser l'opération se dérouler ;
- bloquer l'opération et exécuter les actions spécifiées dans les paramètres de la protection ou d'analyse.

L'interception des événements prend du temps à traiter, ce qui affecte les performances d'autres applications et du système d'exploitation.

Si votre système d'exploitation prend en charge la technologie fanotify et satisfait aux exigences, configurez le module de noyau mis à jour pour l'application. Le module de noyau mis à jour est inclus avec l'application. Le module de noyau mis à jour permet d'optimiser l'interception des opérations sur les fichiers.

Pour exclure les fichiers d'un répertoire donné non seulement de l'analyse, mais également de l'interception, configurez l'exclusion des points de montage (exclusions globales). L'exclusion des points de montage vous permet d'exclure les répertoires locaux ou distants montés sur l'appareil de l'interception des opérations sur les fichiers.

Vous pouvez consulter la liste des points de montage détectés sur l'appareil à l'aide de Web Console, de la Console d'administration ou de la ligne de commande. La liste affiche des informations indiquant si le point de montage a été ajouté aux exclusions de l'analyse.

Les experts de Kaspersky recommandent d'utiliser des exclusions globales si :

- la connexion à une ressource distante montée, telle que NFS ou SMB, est lente ;
- Même les retards minimes dans le fonctionnement du système sont critiques.

Vous pouvez spécifier le type de point de montage (Local, AllRemoteMounted, Mounted:NFS, Mounted:SMB ou Mounted:Custom) ou des points de montage spécifiques. L'application ne surveille pas les zones exclues.

Pour protéger les ressources réseau partagées, utilisez l'application Kaspersky Endpoint Security sur l'appareil sur lequel les ressources sont physiquement stockées.

Si vous utilisez le module de noyau mis à jour pour l'interception des événements système, vous pouvez exclure de l'interception des répertoires locaux ou distants particuliers montés sur l'appareil, et pas uniquement des points de montage entiers.

Si vous utilisez fanotify pour l'interception des événements système, les exclusions globales ne s'appliquent pas aux chemins qui ne sont pas des points de montage.

Vous pouvez configurer des exclusions globales dans une stratégie à l'aide de Web Console ou de la Console d'administration, ou localement sur l'appareil à l'aide de la ligne de commande.

Exemple d'exclusion globale configurée pour le répertoire /tmp à l'aide de la ligne de commande

Pour exclure tous les fichiers du répertoire /tmp de l'interception :

1. Si vous utilisez fanotify pour l'interception des événements système, vérifiez si le répertoire /tmp est un point de montage :

   ```
   mount
   ```

   Si le répertoire est absent de la sortie de la commande mount :

   a. Créez un point de montage :

      ```
      mount --bind /tmp/ /tmp
      ```

   b. Ajoutez la ligne suivante au fichier /etc/fstab afin que le point de montage nouvellement créé soit conservé dans le système après le redémarrage :

      ```
      /tmp /tmp none defaults,bind 0 0
      ```

   Si vous utilisez le module de noyau mis à jour pour l'interception des événements système, ignorez cette étape.

2. Ajoutez le répertoire /tmp aux exclusions globales :

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

3. Redémarrez l'application pour appliquer les exclusions globales :

   ```
   systemctl restart kesl
   ```

Limitation de l'utilisation de la RAM par l'application

Vous pouvez limiter la quantité de RAM utilisée par Kaspersky Endpoint Security lors de l'analyse des fichiers avec le module Protection contre les fichiers malicieux et lors de l'exécution de tâches d'analyse de type ODS et ContainerScan.

Les limites d'utilisation de la mémoire peuvent être utiles pour les systèmes dotés de grandes quantités de la mémoire vive (plus de 5 Go).

Par défaut, la limite d'utilisation de la mémoire de l'application est de 8 192 Mo. Vous pouvez ajuster la quantité de RAM utilisée par l'application :

- Dans la stratégie, utilisez le paramètre **Limite d'utilisation de la mémoire pour les tâches d'analyse (Mo)**.
- Localement sur l'appareil à l'aide du paramètre `ScanMemoryLimit` dans le fichier de configuration kesl.ini.

Si la valeur spécifiée du paramètre est inférieure à 2 Mo, l'application utilise la valeur minimale (2 Mo). Si la valeur spécifiée du paramètre est supérieure à la quantité de mémoire vive de l'appareil, l'application utilisera au maximum 25 % de la mémoire vive. Vous ne pouvez pas modifier cette valeur.

Ce paramètre limite uniquement la quantité de mémoire utilisée lors de l'analyse des fichiers. Cela signifie que la quantité totale de mémoire requise par l'application peut être supérieure à la valeur de ce paramètre.

Recommandations supplémentaires pour la Protection contre les fichiers malicieux

Analyser uniquement à l'ouverture d'un fichier

Modifier le mode d'analyse des fichiers afin que l'analyse soit effectuée uniquement lorsqu'un fichier est ouvert. Par défaut, l'application vérifie le fichier lorsque vous essayez de l'ouvrir et à nouveau lorsque vous essayez de le fermer si le fichier a été modifié.

Vous pouvez modifier le mode d'analyse des fichiers dans les paramètres de la Protection contre les fichiers malicieux :

- Dans la stratégie utilisant Web Console ou la Console d'administration : définissez la valeur **À l'accès** pour le paramètre **Mode de la Protection contre les fichiers malicieux**.
- Localement sur l'appareil :

```
kesl-control --set-set 1 ScanByAccessType=Open
```

Les modifications introduites dans le fichier après l'ouverture ne seront pas analysées avant la prochaine consultation du fichier.

Analyse des archives

Assurez-vous que l'analyse des archives est désactivée (paramètre par défaut). L'analyse des archives réduit les performances du fait que l'accès au fichier d'archive est bloqué avant que le fichier ne soit décompressé dans un répertoire /tmp temporaire et analysé. Les archives comprennent à la fois des archives traditionnelles et des objets compactés de type .jar.

Vous pouvez activer ou désactiver l'analyse des archives à l'aide de Web Console ou de la Console d'administration (paramètre **Analyser les archives**) ou localement sur l'appareil à l'aide de la ligne de commande (paramètre `ScanArchived`).

Analyse des fichiers copiés depuis des répertoires réseau

Configurez une exclusion de l'analyse pour les fichiers copiés depuis des répertoires réseau. L'analyse des fichiers aura lieu uniquement après la fin de la copie dans le répertoire local.

Pour exclure de l'analyse les fichiers des répertoires réseau, vous devez configurer une exclusion de processus pour l'utilitaire destiné à copier les fichiers depuis les répertoires réseau (par exemple, pour l'utilitaire `cp`).

Si vous gérez une application à l'aide de Kaspersky Security Center, vous pouvez configurer l'exclusion par processus dans Web Console ou dans la Console d'administration. Si vous gérez votre application à l'aide de la ligne de commande, vous pouvez configurer l'exclusion par processus en ajoutant la section [ExcludedForProgram.item_#] aux `[ExcludedForProgram.item_#]` de type OAS.

Recommandations supplémentaires pour les tâches d'analyse

Planification du lancement de la tâche

Configurez un calendrier d'exécution des tâches d'analyse afin que les tâches s'exécutent à des moments différents. L'application vous permet d'exécuter des tâches d'analyse simultanément, mais la consommation de ressources peut augmenter considérablement. Vérifiez la planification de toutes les tâches de types ODS et ContainerScan localement sur l'appareil ou via Kaspersky Security Center.

Lancez l'analyse quand le serveur est soumis à la charge la moins importante.

Analyse des répertoires distants

Assurez-vous que la zone des tâches d'analyse n'inclut aucun répertoire distant monté sur l'appareil via SMB ou NFS.

Il est recommandé de vérifier ces répertoires directement sur l'appareil fournissant la ressource. Si cela n'est pas possible, n'effectuez pas l'analyse sur les serveurs avec des services critiques, car une telle tâche peut prendre beaucoup de temps (en fonction de la vitesse de connexion et du nombre de fichiers).

Utilisation des exclusions globales et des exclusions de la Protection contre les fichiers malicieux

Assurez-vous que les paramètres suivants sont activés pour la tâche d'analyse des logiciels malveillants :

- **Utiliser les exclusions globales** (`UseGlobalExclusions`) pour exclure de l'analyse les points de montage spécifiés dans les exclusions globales.
- **Utiliser les exclusions de la Protection contre les fichiers malicieux** (`UseOASExclusions`) pour utiliser les exclusions configurées de la Protection contre les fichiers malicieux pendant l'analyse.

Par défaut, les deux paramètres sont activés.

Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez définir `/.snapshots/*/snapshot/` en tant que chemin d'exclusion.

Recommandations pour la Protection contre les menaces Internet et la Protection contre les menaces réseau

Recommandations générales

Pare-feu du système d'exploitation

Si le système dispose de ses propres règles réseau (ou règles firewalld) avec des stratégies Drop, pour que l'application fonctionne correctement, ajoutez une règle d'acceptation afin d'autoriser les connexions entrantes depuis l'appareil local (loopback) :

Exemple de commande pour iptables

```
iptables -A INPUT -i lo -j ACCEPT
```

Liste des ports réseau contrôlés

Limitez la liste des ports réseau contrôlés par l'application. Par défaut, l'application surveille uniquement les ports réseau sélectionnés. Si l'appareil utilise une connexion SMB, assurez-vous que la valeur par défaut est utilisée :

- Dans la stratégie de Web Console ou dans la Console d'administration : sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés** dans les paramètres d'analyse du trafic réseau.
- Localement sur l'appareil : le paramètre d'analyse du trafic réseau `MonitorNetworkPort` est défini sur `Selected`.

Utilisation de l'application avec HAProxy

Lorsque vous utilisez l'application avec l'équilibreur de charge HAProxy :

1. Ouvrez le fichier de configuration /var/opt/kaspersky/kesl/common/kesl.ini, créez la section `[Environment]` et ajoutez-y le paramètre `TcpSynInterceptDisabled=1`.
2. Redémarrez l'application :

   ```
   systemctl restart kesl
   ```

Utilisation de l'application avec Kubernetes

Pour que les modules Protection contre les menaces Internet et Protection contre les menaces réseau fonctionnent avec le cluster Kubernetes doté des plug-ins réseau Calico et Cilium, gérez les paramètres `WtpFwMark`, `NtpFwMark`, `BypassFwMark` et `BypassNflogMark` dans le fichier de configuration kesl.ini.

Que faire si l'erreur « Échec de la vérification de l'intégrité du module de l'application » s'affiche

Recommandations pour la Protection contre les menaces Internet

Stratégie de vérification du certificat

Par défaut, le module Protection contre les menaces Internet décrypte et inspecte le trafic réseau transmis via des connexions chiffrées. Dans ce cas, le module peut utiliser Internet pour vérifier et télécharger les chaînes manquantes nécessaires à la vérification du certificat.

Si l'appareil ne dispose pas d'un accès direct à Internet, effectuez l'une des actions suivantes :

- Sélectionnez une méthode locale de validation des certificats dans les paramètres d'analyse du trafic réseau :
  - Dans la stratégie utilisant Web Console ou la Console d'administration : définissez la valeur **Vérification locale** pour le paramètre **Stratégie de vérification du certificat**.
  - Localement sur l'appareil à l'aide de la ligne de commande :

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  L'application n'utilisera pas Internet pour vérifier les certificats.
- Configurez l'accès à Internet via un serveur proxy :
  - Dans une stratégie, à l'aide de la Web Console ou de la Console d'administration : configurez les paramètres du proxy.
  - Localement sur l'appareil en utilisant la ligne de commande : exécutez la commande :

    Activer l'utilisation d'un serveur proxy avec authentification

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    Activer l'utilisation d'un serveur proxy sans authentification

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

Recommandations pour la Protection contre les menaces réseau

Compatibilité avec les règles REDIRECT

Pour garantir la compatibilité des règles d'interception du module Protection contre les menaces réseau avec les règles REDIRECT (par exemple, redirection du port 443 vers le port 8443) :

1. Supprimez la règle :

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

2. Remplacez-la par les règles suivantes :

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports
8443
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT
--to-destination :8443
```

Recommandations pour la Détection comportementale

Nous recommandons d'exclure de l'analyse l'activité des processus les plus fréquemment analysés par le module Détection comportementale.

Pour savoir quels processus sont lancés le plus fréquemment, exécutez la commande suivante :

```
kesl-control --get-statistic --processes
```

Cette commande affiche la liste des processus dont Kaspersky Endpoint Security détecte le plus fréquemment le lancement, ainsi que le nombre de lancements de ces processus.

Vous pouvez configurer des exclusions dans une stratégie à l'aide de Web Console ou de la Console d'administration, ou localement sur l'appareil à l'aide de la ligne de commande.

Par défaut, seul le processus indiqué est exclu de l'analyse ; la Détection comportementale continue d'analyser les processus enfants d'un processus exclu.

Exemples de configuration des exclusions en ligne de commande

Exclure de l'analyse l'activité de my_program1 et my_program2

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

Exclure de l'analyse l'activité de my_program1 et de ses processus enfants

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

Interopérabilité avec les solutions Kaspersky

L'application Kaspersky Endpoint Security prend en charge l'interopérabilité avec certaines solutions Kaspersky. Pour une interopérabilité optimale des applications, suivez les recommandations de cette section.

Kaspersky Security Center Linux

Lors de l'utilisation de Kaspersky Endpoint Security for Linux avec Kaspersky Security Center 17.0 Linux, nous vous recommandons d'utiliser les paramètres décrits dans cet article.

Paramètres recommandés

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent` • `/var/lib/postgresql/<PostgreSQL version>`
Analyse des logiciels malveillants	Enabled	Ajoutez les chemins d'accès des répertoires contenant les bases de données aux exclusions globales.
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces réseau	Enabled	Sélectionner le mode d'interception du trafic réseau eBPF `NetInterceptorMode=UseEBPF`
Protection contre les menaces Internet	Enabled	Utiliser les paramètres par défaut.
Protection contre le chiffrement	Désactivé	–
Analyser les conteneurs	Désactivé	–
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Enabled	Ajouter des zones d'analyse : • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
Vérification de l'intégrité du système	Désactivé	–
Endpoint Detection and Response Expert (on-premises)	Enabled	Utiliser les paramètres par défaut.
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Enabled	Utiliser les paramètres par défaut.
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Certaines restrictions s'appliquent	Pour les actions de réponse, vous ne pouvez pas exclure les objets requis par Kaspersky Endpoint Security for Linux, ni les objets système critiques. Lorsque vous lancez des actions de réponse, assurez-vous qu'elles ne perturbent pas le système et les applications que vous utilisez.

Module de l'application	État recommandé du module	Recommandations
Interface graphique	Non défini	–
plug-in Internet d'administration de Kaspersky Endpoint Security for Linux	Installée	Utiliser les paramètres par défaut.
plug-in MMC d'administration de Kaspersky Endpoint Security for Linux	Installée	Utiliser les paramètres par défaut.
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Enabled	Utiliser les paramètres par défaut.
Protection BadUSB	Désactivé	–
Exclusions globales	Configuré	Si vous installez Kaspersky Security Center à l'aide du script d'installation rapide, ajoutez les points de montage aux exclusions : `/var/lib/postgresql/<PostgreSQL version>/main` où `<PostgreSQL version>` est le numéro de la version du SGBD PostgreSQL que vous utilisez.

Kaspersky Unified Monitoring and Analysis Platform

Lors de l'utilisation de Kaspersky Endpoint Security for Linux avec les versions 4.2 et 4.6 de Kaspersky Unified Monitoring and Analysis Platform déployées dans un cluster Raft, nous vous recommandons d'utiliser les paramètres décrits dans cet article.

Paramètres recommandés

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
Analyse des logiciels malveillants	Désactivé	–
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Exclure le processus de l'analyse `/opt/kaspersky/kuma`
Protection contre les menaces réseau	Enabled	Désactiver le blocage de l'appareil compromis `BlockAttackingHosts=No`
Protection contre les menaces Internet	Désactivé	–
Protection contre le chiffrement	Désactivé	–
Analyser les conteneurs	Désactivé	–

Module de l'application	État recommandé du module	Recommandations
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Désactivé	–
Vérification de l'intégrité du système	Désactivé	–
Endpoint Detection and Response Expert (on-premises)	Désactivé	–
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Désactivé	–
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Désactivé	–
Interface graphique	Non défini	–
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Désactivé	–
Protection BadUSB	Désactivé	–

Référence des modules de l'application

Commandes de gestion de Kaspersky Endpoint Security

L'application Kaspersky Endpoint Security est gérée à partir de la ligne de commande à l'aide des commandes de gestion de Kaspersky Endpoint Security.

Vous pouvez afficher l'aide sur les commandes de gestion à l'aide de la commande :

```
kesl-control --help <prefix of command group>
```

où `<prefix of command group>` peut prendre les valeurs suivantes :

- `-A` : commandes de gestion du Contrôle des applications
- `-B` : commandes de gestion de la Sauvegarde
- `-C` : commandes de gestion des paramètres généraux d'analyse du conteneur
- `-D` : commandes de gestion du Contrôle des appareils
- `-E` : commandes permettant d'afficher les événements actuels de l'application
- `-F` : commandes de Gestion du pare-feu
- `-H` : commandes permettant de gérer les appareils bloqués par la Protection contre le chiffrement et la Protection contre les menaces réseau
- `-J` : commandes de gestion de la collecte des métriques de performances système
- `-L` : commandes de gestion des clés de licence
- `-M` : commandes de gestion des paramètres d'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform
- `-N` : commandes de gestion des paramètres d'analyse des connexions chiffrées
- `-Q` : commandes de gestion de la Quarantaine
- `-R` : commandes permettant de gérer les paramètres d'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (cloud) et Kaspersky Endpoint Detection and Response Optimum
- `-S` : commandes statistiques.
- `-T` : commandes de gestion des tâches et paramètres de l'application
- `-U` : commandes de gestion des utilisateurs et rôles

- `-V` : commandes de l'application en mode Light Agent
- `-W` : commandes permettant d'afficher les événements du journal des événements de l'application
- `-X` : commandes de gestion des paramètres d'intégration de l'application Kaspersky Endpoint Security avec Sandbox

Dans le shell bash, vous pouvez activer la saisie semi-automatique pour les commandes kesl-control.

```
Activer la saisie semi-automatique pour la commande kesl-control dans la session bash actuelle
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

```
Activer la saisie semi-automatique pour toutes les nouvelles sessions bash
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Commandes de gestion des clés de licence

Le préfixe `-L` indique que la commande appartient au groupe de commandes utilisées pour gérer les clés de licence.

> Les commandes d'ajout ou de suppression de clés de licence peuvent être utilisées si l'application fonctionne en mode standard ou en mode EDR Agent. Si l'application est utilisée en mode Light Agent, les commandes de gestion des clés renvoient une erreur.

Commande kesl-control --add-active-key

La commande vous permet d'ajouter une clé de licence active à l'application à l'aide d'un fichier de clé ou d'un code d'activation.

Vous pouvez utiliser ces commandes pour ajouter des clés afin d'activer l'application ou des modules qui ne sont pas couverts par votre licence. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

```
Ajouter une clé de licence à l'aide d'un fichier clé
kesl-control [-L] --add-active-key <key file path>
```

```
Ajouter une clé de licence à l'aide d'un code d'activation
kesl-control [-L] --add-active-key <activation code>
```

Où :

`<key file path>` est le chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.

<activation code> est le code d'activation.

Exemple d'ajout d'une clé à l'aide du fichier /home/test/00000001.key comme clé active

```
kesl-control --add-active-key /home/test/00000001.key
```

Commande kesl-control --add-reserve-key

La commande vous permet d'ajouter une clé de licence de réserve à l'application à l'aide d'un fichier clé ou d'un code d'activation.

Vous pouvez utiliser ces commandes pour ajouter des clés afin d'activer l'application ou des modules qui ne sont pas couverts par votre licence. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

> Si la clé active n'a pas encore été ajoutée à l'application sur l'appareil, la commande échoue.

Ajouter une clé de licence de réserve à l'aide d'un fichier clé

```
kesl-control [-L] --add-reserve-key <key file path>
```

Ajouter une clé de licence de réserve à l'aide d'un code d'activation

```
kesl-control [-L] --add-reserve-key <activation code>
```

Où :

<key file path> est le chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.

<activation code> est le code d'activation.

Exemple d'ajout d'une clé de réserve à l'aide du fichier /home/test/00000002.key

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Commande kesl-control --remove-active-key

La commande permet de supprimer une clé de licence active.

Supprimer la clé de licence EDR Optimum active

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Supprimer la clé de licence KUMA active

```
kesl-control [-L] --remove-active-key [--kuma]
```

Supprimer la clé de licence MDR active

```
kesl-control [-L] --remove-active-key [--mdr]
```

Supprimer la clé de licence EDR Expert (on-premises) active

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

Supprimer la clé de licence EDR Expert (cloud) active

```
kesl-control [-L] --remove-active-key [--cxdr]
```

Supprimer la clé de licence KWSM active

```
kesl-control [-L] --remove-active-key [--khcs]
```

Où :

`--edr-optimum` : supprimer la clé de licence active EDR Optimum.

`--kuma` : supprimer la clé de licence KUMA active.

`--mdr` : supprimer la clé de licence MDR active.

`--edr-kata` – supprimer la clé de licence EDR Expert (on-premises) active.

`--cxdr` – supprimer la clé de licence EDR Expert (cloud) active.

`--khcs` : supprimer la clé de licence KWSM active.

Si vous ne spécifiez pas l'option `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` ou `--khcs` dans la ligne de commande, la commande supprime la clé active avec laquelle votre application est activée.

Commande kesl-control --remove-reserve-key

La commande vous permet de supprimer la clé de licence de réserve.

Supprimer la clé de licence de réserve EDR Optimum

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

Supprimer la clé de licence de réserve KUMA

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

Supprimer la clé de licence de réserve MDR

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

Supprimer la clé de licence de réserve EDR Expert (on-premises)

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Supprimer la clé de licence de réserve EDR Expert (cloud)

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

Supprimer la clé de licence de réserve KWSM

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

Où :

`--edr-optimum` : supprimer la clé de licence de réserve EDR Optimum.

`--kuma` : supprimer la clé de licence de réserve KUMA.

`--mdr` : supprimer la clé de licence de réserve MDR.

`--edr-kata` – supprimer la clé de licence de réserve EDR Expert (on-premises).

`--cxdr` – supprimer la clé de licence de réserve EDR Expert (cloud).

`--khcs` : supprimer la clé de licence de réserve KWSM.

Si vous ne spécifiez pas l'option `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` ou `--` dans la ligne de commande, la commande supprime la clé de réserve de l'application.

Commande kesl-control -L --query

La commande affiche des informations sur la licence utilisée pour activer l'application et sur les clés de licence actuellement utilisées.

```
kesl-control -L --query [--json]
```

Où :

`--json` : afficher les données au format JSON.

Commande kesl-control --load-mdr-blob

La commande permet de télécharger un fichier BLOB sur l'appareil, qui peut être utilisé pour l'intégration avec Kaspersky Managed Detection and Response. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR.

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

Commande kesl-control --remove-mdr-blob

La commande permet de supprimer de l'appareil le fichier BLOB utilisé pour l'intégration avec Kaspersky Managed Detection and Response.

```
kesl-control [-L] --remove-mdr-blob
```

Commandes de gestion des utilisateurs et des rôles

-U : préfixe qui indique que la commande appartient au groupe de commandes pour l'administration des utilisateurs et des rôles.

Gestion des rôles des utilisateurs

Afficher une liste d'utilisateurs et de rôles

```
kesl-control [-U] --get-user-list
```

Attribuer un rôle à l'utilisateur spécifié

```
kesl-control [-U] --grant-role <role> <user>
```

Révoquer un rôle d'utilisateur

```
kesl-control [-U] --revoke-role <role> <user>
```

Où :

`<user>` est le nom d'un utilisateur ou d'un groupe d'utilisateurs.

`<role>` est le rôle d'un utilisateur ou d'un groupe d'utilisateurs.

Paramètres de la Protection par mot de passe

Vous pouvez utiliser des commandes pour gérer la Protection par mot de passe.

Activer ou désactiver la Protection par mot de passe

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

Consulter les paramètres actuels de la Protection par mot de passe

```
kesl-control --get-permission-manager-settings
```

Modifier les autorisations d'un utilisateur ou d'un groupe

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

Consulter les autorisations actuelles d'un utilisateur ou d'un groupe

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

Supprimer un utilisateur ou un groupe d'utilisateurs dont les autorisations sont configurées

```
kesl-control --remove-permissions <user> [--group]
```

Où :

`<user>` est le nom d'un utilisateur ou d'un groupe d'utilisateurs.

`<permissions>` correspond aux autorisations personnalisées.

`--group` applique le paramètre à un groupe d'utilisateurs. Si cette option n'est pas spécifiée, le paramètre s'applique à un utilisateur individuel.

`--file <path to file>` enregistre ou exporte les paramètres dans un fichier de configuration. Si cette option n'est pas spécifiée, le résultat de la commande est écrit sur la sortie standard.

`--json` : afficher les paramètres au format JSON.

Gestion de la stratégie sur l'appareil

> Pour désactiver la stratégie sur un appareil, l'utilisateur doit disposer de l'autorisation Désactiver la stratégie de Kaspersky Security Center.

Si l'utilisateur a désactivé la stratégie sur l'appareil, la stratégie redevient active après le redémarrage de l'appareil ou de Kaspersky Endpoint Security.

Désactiver la stratégie sur l'appareil

```
kesl-control --disable-policy
```

Appliquer la stratégie à l'appareil

```
kesl-control --enable-policy
```

Gestion des tâches et des paramètres de l'application

Le préfixe `-T` indique que la commande appartient au groupe de commandes de gestion des paramètres et des tâches de l'application.

Le préfixe `-C` indique que la commande appartient au groupe de commandes de gestion des paramètres de l'Analyse du conteneur.

Le préfixe `-N` indique que la commande appartient au groupe de commandes de gestion des paramètres d'analyse du trafic réseau.

Commande kesl-control --export-settings

Cette commande affiche tous les paramètres de l'application dans la console ou les exporte vers un fichier de configuration. Cela comprend les paramètres généraux de l'analyse du conteneur, les paramètres d'analyse des connexions chiffrées, les paramètres généraux de l'application et les paramètres des tâches.

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

Où :

`--file <path to file>` est le chemin d'accès complet au fichier de configuration dans lequel vous souhaitez enregistrer les paramètres de l'application.

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --import-settings

Accordez l'accès au fichier de configuration uniquement aux utilisateurs de confiance. Avant d'importer les paramètres dans l'application, vérifiez les chemins d'accès aux répertoires, aux fichiers de configuration, aux fichiers exécutables et à la quarantaine. N'importez pas de fichiers de configuration provenant de sources non fiables. La compromission du fichier de configuration pourrait affecter la sécurité, l'intégrité ou le fonctionnement de l'infrastructure de votre organisation, ainsi que les données des utilisateurs.

La commande vous permet d'importer tous les paramètres de l'application à partir du fichier de configuration (y compris les paramètres généraux de l'analyse du conteneur, les paramètres de l'analyse des connexions sécurisées, les paramètres généraux de l'application et les paramètres des tâches).

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

Où :

`--file <path to file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de l'application.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --update-application

Cette commande installe une mise à jour du module de l'application téléchargée.

La commande ne peut pas être exécutée si l'application est utilisée en mode Light Agent.

```
kesl-control [-T] --update-application
```

Commandes de gestion des paramètres généraux de l'application

kesl-control --get-app-settings

La commande vous permet d'afficher les valeurs actuelles des paramètres généraux de l'application sur la console ou le fichier de configuration.

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

Où :

`--file <path to file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres généraux de l'application. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON.

kesl-control --set-app-settings

La commande vous permet de définir les valeurs des paramètres généraux de l'application à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

```
Spécifiez les paramètres à l'aide des options de ligne de commande :
```

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Spécifiez les paramètres à l'aide d'un fichier de configuration :
```

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

Où :

`<setting name>=<setting value>` correspond au nom et à la valeur d'un paramètre général de l'application.

`--file <path to file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de l'application.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des paramètres des tâches

Commande kesl-control --get-settings

La commande vous permet d'afficher les valeurs actuelles des paramètres de la tâche spécifiée sur la console ou le fichier de configuration.

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`--file <path to file>` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de la tâche. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --set-settings

La commande vous permet de définir les valeurs des paramètres de la tâche spécifiée à l'aide des touches de commande ou en important des paramètres à partir d'un fichier de configuration spécifié.

Spécifiez les paramètres à l'aide des options de ligne de commande :

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

Spécifiez les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`<setting name>=<setting value>` correspond au nom et à la valeur d'un paramètre de tâche.

`--add-path <path>` ajoute un chemin d'accès à un répertoire contenant les objets à analyser.

`--del-path <path>` supprime un chemin d'accès à un répertoire contenant les objets à analyser.

`--add-exclusion <path>` ajoute un chemin d'accès à un répertoire contenant les objets à exclure de l'analyse.

`--del-exclusion <path>` supprime le chemin d'accès au répertoire contenant les objets à exclure de l'analyse.

`--file <path to file>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de la tâche.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --set-to-default

La commande vous permet de restaurer les valeurs par défaut des paramètres de la tâche spécifiée.

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

kesl-control --get-schedule

La commande permet d'afficher le planification de lancement actuel de la tâche spécifiée dans la console ou dans un fichier de configuration.

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`--file <path to file>` correspond au chemin d'accès au fichier de configuration dans lequel vous souhaitez exporter les paramètres de planification de la tâche. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON.

kesl-control --set-schedule

La commande vous permet de définir la planification d'une tâche spécifiée à l'aide des touches de commande ou en important des paramètres à partir d'un fichier de configuration spécifié.

Spécifiez les paramètres à l'aide des options de ligne de commande :

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Spécifiez les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`<setting name>=<setting value>` correspond au nom et à la valeur d'un paramètre de planification des tâches.

`--file <path to file>` correspond au chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres de planification de la tâche.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des tâches

Commande kesl-control --get-task-list

Cette commande affiche la liste des tâches existantes.

```
kesl-control [-T] --get-task-list [--json]
```

Où :

`--json` : afficher les paramètres au format JSON.

Les informations suivantes sont affichées pour chaque tâche :

- `Name` : nom de la tâche.
- `ID` : identifiant de la tâche.

- `Type` : type de tâche.
- `State` : état actuel de la tâche

Si la stratégie de Kaspersky Security Center empêche les utilisateurs de consulter ou de modifier les tâches locales, les informations relatives aux tâches `Scan_My_Computer`, `Critical_Areas_Scan`, `Container_Scan`, `Inventory_Scan`, `Update` (en mode standard) et `Rollback` (en mode standard) ne sont pas disponibles.

Commande kesl-control --get-task-state

Cette commande renvoie l'ID de la tâche créée.

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`--json` : afficher les paramètres au format JSON.

Les tâches de l'application peuvent prendre les états suivants :

- `Started` : en cours d'exécution.
- `Starting` : en cours de démarrage.
- `Stopped` : tâche arrêtée.
- `Stopping` : en cours d'arrêt.

Les tâches des types `ODS`, `ODFIM` et `InventoryScan` peuvent également avoir l'un des états suivants :

- `Pausing` : en cours de suspension.
- `Suspended` : suspendue.
- `Resuming` : en cours de reprise.

Commande kesl-control --create-task

Cette commande crée une tâche du type spécifié avec les paramètres par défaut ou les paramètres spécifiés dans un fichier de configuration.

Seules les tâches définies par l'utilisateur peuvent être créées ou supprimées. Les tâches prédéfinies ne peuvent pas être créées ni supprimées.

Selon le mode de fonctionnement de l'application, vous pouvez créer les types suivants de tâches définies par l'utilisateur :

- Mode standard : `ODS`, `Update`, `Rollback`, `ODFIM`, `ContainerScan` et `InventoryScan`.
- Mode Light Agent : `ODS`, `ODFIM`, `ContainerScan` et `InventoryScan`.

Créer une tâche avec les paramètres par défaut

```
kesl-control [-T] --create-task <task name> --type <task type>
```

Créer une tâche avec les paramètres repris d'un fichier de configuration

```
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

Où :

`<task name>` est le nom que vous avez spécifié pour une nouvelle tâche.

`<task type>` indique le type de tâche que vous souhaitez créer.

`--file <path to file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres qui seront utilisés pour créer la tâche.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --delete-task

Cette commande supprime une tâche.

Seules les tâches définies par l'utilisateur peuvent être créées ou supprimées. Les tâches prédéfinies ne peuvent pas être supprimées.

```
kesl-control [-T] --delete-task <task ID|name>
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

Commande kesl-control --start-task

Cette commande supprime une tâche.

Vous pouvez démarrer et arrêter toutes les tâches prédéfinies et les tâches définies par l'utilisateur, à l'exception des tâches de type `License`.

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`-W` – activer l'affichage des événements en cours.

`--progress` : afficher la progression de la tâche.

```
Exemple d'exécution d'une tâche avec l'identifiant 1 et d'activation de l'affichage des événements en cours associés à la tâche
```

```
kesl-control --start-task 1 -W
```

Si une erreur se produit lors du démarrage d'une tâche et que la tâche ne démarre pas, une fois l'application redémarrée, une nouvelle tentative de démarrage de la tâche est effectuée.

Commande kesl-control --stop-task

Cette commande supprime une tâche.

Vous pouvez démarrer et arrêter toutes les tâches prédéfinies et les tâches définies par l'utilisateur, à l'exception des tâches de type `License`.

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

`-W` – activer l'affichage des événements en cours.

Commande kesl-control --suspend-task

Cette commande supprime une tâche.

Vous pouvez uniquement suspendre les tâches `ODS`, `ODFIM` et `InventoryScan`.

```
kesl-control [-T] --suspend-task <task ID|name>
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

Commande kesl-control --resume-task

Cette commande supprime une tâche.

Vous pouvez uniquement reprendre les tâches `ODS`, `ODFIM` et `InventoryScan`.

```
kesl-control [-T] --resume-task <task ID|name>
```

Où :

`<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.

Commande kesl-control --scan-file

La commande vous permet de créer et d'exécuter une tâche d'analyse personnalisée.

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

Où :

`<path>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

`--action <action>` est l'action que vous souhaitez que l'application effectue sur les objets infectés. Si vous ne spécifiez pas la clé `--action` , l'application effectuera l'action recommandée.

Commande kesl-control --scan-container my_container

La commande vous permet de créer et d'exécuter une tâche d'analyse personnalisée du conteneur ou de l'image.

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

Où :

`<ID|name[:tag]>` est le nom ou l'identifiant du conteneur ou de l'image. Vous pouvez utiliser des masques pour analyser plusieurs objets.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Commandes de gestion des paramètres généraux d'analyse du conteneur

kesl-control --get-container-settings

La commande permet d'afficher les valeurs actuelles des paramètres généraux de l'analyse du conteneur dans la console ou dans un fichier de configuration.

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

Où :

`--file <path to file>` est le chemin d'accès au fichier de configuration vers lequel vous souhaitez exporter les paramètres généraux de l'Analyse du conteneur. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON.

kesl-control --set-container-settings

La commande vous permet de définir les valeurs des paramètres généraux de l'analyse du conteneur à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

Spécifiez les paramètres à l'aide des options de ligne de commande :

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Spécifiez les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

Où :

`<setting name>=<setting value>` est le nom et la valeur d'un paramètre général de l'Analyse du conteneur.

`--file <path to file>` est le chemin d'accès complet au fichier de configuration depuis lequel vous souhaitez importer les paramètres généraux de l'Analyse du conteneur.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des paramètres d'analyse du trafic réseau

Le préfixe `-N` indique que la commande appartient au groupe de commandes de gestion des paramètres d'analyse du trafic réseau.

Commande kesl-control -N --query

La commande permet d'afficher des listes d'exclusions à l'analyse des connexions chiffrées :

- liste des exclusions ajoutées par l'utilisateur ;
- liste des exclusions ajoutées par l'application ;
- une liste des exclusions reçues des bases de données de l'application.

```
Afficher la liste des exclusions ajoutées par l'utilisateur
```

```
kesl-control -N --query user
```

```
Afficher la liste des exclusions ajoutées par l'application
```

```
kesl-control -N --query auto
```

```
Afficher la liste des exclusions reçues des bases de données de l'application
```

```
kesl-control -N --query kl
```

Commande kesl-control --clear-web-auto-excluded

La commande vous permet d'effacer la liste des domaines que l'application a automatiquement exclus de l'analyse.

```
kesl-control -N --clear-web-auto-excluded
```

Commande kesl-control --get-net-settings

La commande permet d'afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à la console ou à un fichier de configuration.

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

Où :

`--file <path to file>` est le chemin d'accès au fichier de configuration dans lequel vous voulez exporter les paramètres d'analyse du trafic réseau. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --set-net-settings

La commande vous permet de définir les valeurs des paramètres d'analyse du trafic réseau à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

Spécifiez les paramètres à l'aide des options de ligne de commande :

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Spécifiez les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

Où :

`<setting name>=<setting value>` est le nom et la valeur d'un paramètre d'analyse du trafic réseau.

`--file <path to file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous voulez importer les paramètres d'analyse du trafic réseau.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --list-certificates

La commande permet d'afficher une liste des certificats racines de confiance.

```
kesl-control [-N] --list-certificates
```

Commande kesl-control --add-certificate

La commande vous permet d'ajouter un certificat à la liste des certificats racines de confiance.

```
kesl-control [-N] --add-certificate <path to certificate>
```

Où :

`<path to certificate>` est le chemin d'accès au fichier de certificat que vous voulez ajouter (au format PEM ou DER).

Commande kesl-control --remove-certificate

La commande permet de supprimer un certificat de la liste des certificats racines de confiance.

```
kesl-control [-N] --remove-certificate <certificate subject>
```

Commande kesl-control --add-bypass-endpoints

La commande vous permet d'ajouter une exclusion à l'interception du trafic.

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Où :

`<in|out>` est la direction du trafic dans la connexion exclue, sortant ou entrant.

`<remote IP address>` est l'adresse IPv4 ou IPv6 de l'appareil distant. Lors de l'exclusion du trafic entrant de l'interception, le trafic provenant de l'adresse IP spécifiée sera exclu. Lors de l'exclusion du trafic sortant de l'interception, le trafic vers l'adresse IP spécifiée sera exclu.

`<destination port>` est un port sur l'appareil protégé (exclusion pour le trafic entrant) ou un port sur l'appareil distant (exclusion pour le trafic sortant). Le trafic vers ce port est exclu de l'interception.

Commande kesl-control --list-bypass-endpoints

La commande vous permet de consulter la liste des exclusions configurées à partir de l'interception du trafic.

```
kesl-control [-N] --list-bypass-endpoints
```

Commande kesl-control --remove-bypass-endpoints

La commande vous permet de supprimer une exclusion à l'interception du trafic.

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Où :

`<in|out>` est la direction du trafic dans la connexion exclue, sortant ou entrant.

`<remote IP address>` est l'adresse IPv4 ou IPv6 de l'appareil distant dont le trafic est exclu de l'interception (selon la direction du trafic).

`<destination port>` est un port sur l'appareil protégé (exclusion pour le trafic entrant) ou un port sur l'appareil distant (exclusion pour le trafic sortant).

Surveillance de l'état et de la protection

Commandes de statistiques

Le préfixe -S indique que la commande appartient au groupe de commandes statistics.

kesl-control --app-info

La commande permet d'afficher des informations sur l'application.

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

Où :

`--json` : afficher les paramètres au format JSON.

`--check-permissions` affiche les chemins d'accès aux répertoires de l'application dont les autorisations sont configurées de manière incorrecte.

Commande kesl-control --supported-tech-info

Cette commande affiche une liste des fonctions de l'application, des informations sur leur état (utilisées ou non) et les technologies Linux avec lesquelles ces fonctions de l'application sont implémentées.

```
kesl-control [-S] --supported-tech-info [--json]
```

Où :

`--json` : afficher les fonctions au format JSON.

Commande kesl-control --get-statistic

La commande vous permet d'afficher des statistiques sur le fonctionnement de l'application et une liste des points de montage détectés sur l'appareil.

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Où :

`--files` : statistiques sur les fichiers que le module Protection contre les fichiers malicieux analyse le plus souvent et le nombre de fois où le module accède à ces fichiers ;

`--processes` : statistiques sur les processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, et le nombre de ces lancements ;

> L'exclusion de processus de l'analyse par le module Détection comportementale ne les supprime pas des statistiques, mais améliore les performances de Kaspersky Endpoint Security.

`--mountpoints` : liste des points de montage. Dans le résultat, les chemins d'accès aux points de montage sont triés comme suit :

- points de montage statiques, système, de service et autres
- paquets snap montés et points de montage dans leurs espaces de noms
- Points de montage créés par le système de gestion des conteneurs Docker

Vous pouvez spécifier une ou plusieurs clés dans n'importe quelle combinaison, ou vous pouvez ne spécifier aucune clé du tout. Si vous ne spécifiez pas de clés, l'application affichera trois listes : des statistiques sur les fichiers les plus fréquemment analysés, des statistiques sur les processus les plus fréquemment lancés et une liste des points de montage détectés sur l'appareil.

Commande kesl-control --omsinfo

La commande vous permet de créer un fichier JSON pour l'intégration avec Microsoft Operations Management Suite.

```
kesl-control [-S] --omsinfo --file <path to file>
```

Commande d'affichage des événements

Le préfixe `-W` indique une commande permettant d'afficher les événements du journal des événements de l'application.

Commande kesl-control -W

La commande permet l'affichage des événements en cours de l'application. La commande reprend le nom de l'événement et les informations supplémentaires sur l'événement. Vous pouvez utiliser la commande pour afficher tous les événements de l'application en cours ou uniquement les événements associés à une tâche en cours d'exécution.

```
kesl-control -W [--query "<filter conditions>"]
```

Où :

`<filter conditions>` spécifie une ou plusieurs expressions logiques au format `<field> <comparison operation> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin d'afficher certains événements actuels.

Commandes de gestion des événements de l'application

Le préfixe -E indique que la commande appartient au groupe de commandes utilisé pour gérer les événements de l'application.

Commande kesl-control -E

La commande vous permet d'afficher des informations sur tous les événements du journal des événements de l'application. Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés.

```
kesl-control -E
```

Commande kesl-control -E --query

La commande vous permet d'afficher des informations sur les événements du journal des événements de l'application. Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés. Vous pouvez utiliser un filtre pour afficher des événements spécifiques et également générer une liste d'événements dans un fichier spécifié.

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

Où :

`<database file>` est le chemin complet du fichier de base de données du journal des événements à partir duquel exporter les événements. Par défaut, l'application enregistre les informations relatives aux événements dans la base de données /var/opt/kaspersky/kesl/private/storage/events.db. L'emplacement de la base de données est déterminé par le paramètre général de l'application `EventsStoragePath`.

`<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête.

`<number>` correspond au nombre des événements les plus récents de la sélection (c'est-à-dire au nombre d'enregistrements comptés à partir de la fin de la sélection) que vous souhaitez afficher.

`--file <path to file>` est le chemin complet du fichier dans lequel enregistrer les événements. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.

Si vous ne spécifiez pas la clé `--file` , la liste des événements sera affichée dans la console.

`--json` – afficher les événements au format JSON.

`--reverse` : afficher les événements dans l'ordre inverse (de l'événement le plus récent en haut au plus ancien en bas).

Commande de gestion des métriques de performance du système

Commande kesl-control --export-metrics

La commande vous permet de configurer la collecte des métriques sur l'état du système d'exploitation.

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

Où :

`--period` : affichage périodique des résultats sur la ligne de commande ;

`<interval in seconds between exports>` spécifie la fréquence à laquelle les résultats de la commande sont affichés dans la console de ligne de commande (en secondes)

`--interactive` : affichage interactif (en appuyant sur la touche **Enter**).

Contrôles de sécurité

Commandes de gestion du Contrôle des appareils

Le préfixe -D indique que la commande appartient au groupe de commandes de gestion du Contrôle des appareils.

Gestion des paramètres du Contrôle des appareils

Consulter les paramètres actuels du Contrôle des appareils

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

Modifier les paramètres du Contrôle des applications

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

Où :

`<setting>=<value>` spécifie un paramètre et sa valeur du Contrôle des appareils.

--file <chemin d'accès au fichier> permet d'enregistrer ou d'exporter les paramètres dans un fichier de configuration. Si cette option n'est pas spécifiée, le résultat de la commande est écrit sur la sortie standard.

`--json` : afficher les données au format JSON.

Administration des appareils

Consulter la liste des appareils connectés

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

Où :

`--all` : afficher la liste de tous les appareils connectés.

`--json` : afficher la liste des appareils connectés au format JSON.

`--export <file>` exporte la liste des appareils connectés dans un fichier JSON. La liste des appareils connectés est exportée.

L'application Kaspersky Endpoint Security affiche les informations suivantes sur les appareils connectés :

- **Type d'appareil** Type d'un appareil connecté. Par exemple, `OpticalDrive` ou `HardDrive`.
- **ID**. ID de l'appareil connecté.
- **Nom**. Nom de l'appareil connecté.
- **Chemin d'accès**. Chemin d'accès à l'appareil dans le système d'exploitation virtuel sysfs.
- **Disque système**. Paramètre qui indique si l'appareil connecté est un disque système (oui ou non).
- **Bus**. Bus de connexion. Valeurs possibles : `UnknownBus`, `USB`, `FireWire`.
- **Pilote**. Nom du pilote utilisé, nom lu par le système d'exploitation virtuel sysfs.

Appareils de confiance

Cette commande permet de consulter la liste des appareils de confiance, d'y ajouter et d'en supprimer des appareils, et d'importer une liste d'appareils de confiance à partir d'un fichier.

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

Où :

`--list` : afficher une liste des appareils de confiance.

`--add <ID>` ajoute un appareil à la liste des appareils de confiance par identifiant ou masque d'identifiant d'appareil.

`--delete <ID>` supprime un appareil de la liste des appareils de confiance par identifiant ou masque d'identifiant d'appareil.

`--merge` : fusionner les listes des appareils de confiance lors de l'importation. Si la liste actuelle et la liste importée contiennent des enregistrements pour un appareil ayant le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figurent pas dans la liste actuelle.

`--add` : compléter la liste actuelle des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.

`--replace` : remplacer la liste actuelle des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste importée.

`--file <file>` importe une liste d'appareils de confiance à partir du fichier spécifié. Vous devez spécifier le chemin d'accès complet au fichier au format JSON.

Accès temporaire à un appareil verrouillé

Les commandes permettent de créer un fichier de demande d'accès et de charger une clé d'accès afin d'obtenir un accès temporaire à un appareil bloqué :

Créer un fichier de demande d'accès

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --path <path to access request file>
```

Charger une clé d'accès

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

Où :

`--device-id <device ID>` est l'identifiant de l'appareil verrouillé auquel vous souhaitez accéder.

`--access-duration <access duration>` correspond à la période pendant laquelle vous souhaitez accéder à l'appareil (en heures). Valeurs possibles : 1 à 100.

`--path <path to access request file>` est le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.

`--path <access key>` est le chemin d'accès au fichier contenant la clé d'accès à l'appareil (fichier avec l'extension .acode).

Commandes de gestion du Contrôle des applications

Le préfixe -A indique que la commande appartient au groupe de commandes permettant de gérer le Contrôle des applications.

Gestion de la tâche Inventaire

```
Consulter la liste des applications détectées sur l'appareil client
```

```
kesl-control [-A] --get-app-list [--json]
```

Où :

`--json` : afficher les données au format JSON.

Affichage des catégories d'applications

```
Consulter la liste des catégories créées du Contrôle des applications
```

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to file>] [--json]
```

Où :

`<category name 1> <category name 2> ... <category name N>` sont les noms des catégories. Si vous souhaitez consulter des informations sur plusieurs catégories, saisissez les noms des catégories séparés par un espace.

`--file <path to file>` enregistre ou exporte les paramètres dans un fichier de configuration. Si cette option n'est pas spécifiée, le résultat de la commande est écrit sur la sortie standard.

`--json` : afficher les données au format JSON.

Gestion des catégories d'applications

Pour créer une catégorie d'applications :

1. Écrivez la liste des catégories d'applications dans un fichier de configuration :

```
kesl-control --set-categories --file <path to file>
```

2. Ajoutez les catégories d'applications comme suit :

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

   Pour spécifier le chemin d'accès au fichier dans les champs `Exclude` et `Include`, vous pouvez utiliser des masques.

3. Importez la liste des catégories dans l'application :

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

Modifier la liste des catégories du Contrôle des applications

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

Où :

`FilePath like <application>` est le chemin d'accès complet au fichier exécutable de l'application.

`FileHash == <hash>` est un hachage SHA256 du fichier exécutable de l'application.

`<category ID>` est un ID unique de catégorie. Paramètre obligatoire. Saisissez le `GUID` sans tirets.

`<category name 1> <category name 2> ... <category name N>` sont les noms des catégories. Paramètre obligatoire.

Si vous souhaitez modifier les informations sur plusieurs catégories, spécifiez les noms de catégories séparés par un espace. Si vous n'indiquez pas de nom de catégorie, celle-ci n'est pas créée ou est supprimée de la liste des catégories existantes.

`--file <path to file>` enregistre ou exporte les paramètres dans un fichier de configuration JSON.

Gestion des paramètres du Contrôle des applications

```
Consulter les paramètres actuels du Contrôle des applications
```

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

```
Modifier les paramètres du Contrôle des applications
```

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

Où :

`<setting>=<value>` spécifie un paramètre du Contrôle des applications et sa valeur.

`--file <path to file>` enregistre ou exporte les paramètres dans un fichier de configuration. Si cette option n'est pas spécifiée, le résultat de la commande est écrit sur la sortie standard.

`--json` : afficher les données au format JSON.

Rétablir les paramètres par défaut

```
Supprimer une liste de catégories d'applications et de règles du Contrôle des applications, puis restaurer les paramètres par défaut
```

```
kesl-control --set-settings 21 --set-to-default
```

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Commandes de gestion du Contrôle Internet

Gestion des paramètres de Contrôle Internet

```
Affichage des paramètres actuels de Contrôle Internet :
```

```
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

```
Modification des paramètres de Contrôle Internet
```

```
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

Où :

`<setting>=<value>` est un paramètre de Contrôle Internet et sa valeur. Vous pouvez modifier autant de paramètres que vous le souhaitez.

`--file <path to file>` enregistre ou exporte les paramètres dans un fichier de configuration. Si cette option n'est pas spécifiée, le résultat de la commande est écrit sur la sortie standard.

`--json` : afficher les données au format JSON.

Rétablir les paramètres par défaut

```
Pour supprimer les paramètres configurés et restaurer les paramètres par défaut de Contrôle Internet :
```

```
kesl-control --set-settings 26 --set-to-default
```

Protection des connexions réseau

Commandes de contrôle pour les appareils bloqués

Le préfixe -H indique que la commande appartient au groupe de commandes d'administration des appareils bloqués par la Protection contre le chiffrement et la Protection contre les menaces réseau.

kesl-control --get-blocked-hosts

La commande permet d'afficher une liste des appareils bloqués sur la console.

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

La commande vous permet de déverrouiller les appareils verrouillés.

```
kesl-control [-H] --allow-hosts <address>
```

Où :

`<address>` est une adresse IP d'un appareil ou d'un sous-réseau (IPv4/IPv6, y compris les adresses au format abrégé). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

Commandes de gestion du pare-feu

Le préfixe -F indique que la commande appartient aux commandes Gestion du pare-feu.

Commande kesl-control --add-rule

La commande vous permet d'ajouter une nouvelle règle de paquet réseau.

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

Où :

`--name <rule name>` est le nom de la règle de paquet réseau.

`--action <Allow|Block>` est l'action à réaliser sur les connexions définies dans cette règle de paquet réseau.

`--protocol <protocol>` est le protocole pour lequel vous souhaitez surveiller l'activité réseau.

`--direction <direction>` est la direction de l'activité réseau surveillée.

`--remote <remote address>:<port>` est l'adresse réseau de l'appareil distant.

`--local <local address>:<port>` est l'adresse réseau de l'appareil sur lequel Kaspersky Endpoint Security est installé.

`--at <index>` est le numéro de la règle dans la liste des règles de paquets réseau. Si le commutateur `--at` n'est pas spécifié ou si sa valeur est supérieure au nombre de règles dans la liste, la nouvelle règle est ajoutée à la fin de la liste.

Les paramètres pour lesquels vous ne spécifiez pas de valeurs dans la commande sont définis sur les valeurs par défaut.

Commande kesl-control --del-rule

La commande permet de supprimer une règle de paquet réseau avec le nom spécifié ou avec l'index spécifié dans la liste des règles.

Supprimer une règle de paquet réseau par nom de règle

```
kesl-control [-F] --del-rule --name <rule name>
```

Supprimer une règle de paquet réseau par numéro de règle

```
kesl-control [-F] --del-rule --index <index>
```

Où :

`--name <rule name>` est le nom de la règle de paquet réseau.

`--index <index>` est le numéro de la règle dans la liste des règles de paquets réseau.

Commande kesl-control --move-rule

La commande vous permet de modifier la priorité d'exécution d'une règle de paquet réseau.

Modifier la priorité d'une règle de paquet réseau par nom de règle

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

Modifier la priorité d'une règle de paquet réseau par numéro de règle

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

Où :

`--name <rule name>` est le nom de la règle de paquet réseau.

`--index <index>` est le numéro actuel de la règle dans la liste des règles de paquets réseau.

`--at <index>` est le nouveau numéro de la règle dans la liste des règles de paquets réseau.

Commande kesl-control --add-zone

La commande permet d'ajouter une adresse à une zone réseau.

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

Où :

`--zone <zone>` est le nom prédéfini de la zone réseau.

`--address <address>` est l'adresse réseau ou le sous-réseau.

Commande kesl-control --del-zone

La commande permet de supprimer une adresse de la zone réseau.

Supprimer une adresse d'une zone réseau par adresse ou sous-réseau

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

Supprimer une adresse d'une zone réseau par numéro de règle

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

Où :

`--zone <zone>` est le nom prédéfini de la zone réseau.

`--address <address>` est l'adresse réseau ou le sous-réseau.

`--index <address index>` est le numéro de l'adresse dans la zone réseau.

Commande kesl-control -F --query

La commande vous permet d'afficher les règles de pare-feu créées à l'aide de l'application Kaspersky Endpoint Security.

```
kesl-control -F --query
```

Protection contre les menaces avancées et les attaques ciblées

Commandes de gestion de la quarantaine

Le préfixe -Q indique que la commande appartient au groupe des commandes utilisées pour gérer la quarantaine.

Commande kesl-control -Q --mass-remove

La commande vous permet de supprimer tous les fichiers spécifiés ou uniquement ceux spécifiés de la quarantaine.

Supprimer tous les fichiers

```
kesl-control -Q --mass-remove
```

Supprimer les fichiers qui correspondent aux conditions du filtre

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

Où :

`<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête.

Commande kesl-control --put

La commande est disponible uniquement lorsque Kaspersky Endpoint Security est intégré à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response.

La commande vous permet de mettre un fichier dans la quarantaine.

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

Où :

`<file path>` est le chemin d'accès au fichier que vous souhaitez mettre en quarantaine.

`--md5` : somme de hachage MD5 du fichier que vous souhaitez mettre en quarantaine ;

`--sha256` : somme de hachage SHA256 du fichier que vous souhaitez mettre en quarantaine ;

`--save-original-file` : ne pas supprimer le fichier d'origine. Si vous ne spécifiez pas cette clé, le fichier d'origine sera supprimé.

Commande kesl-control -Q --query

La commande vous permet d'afficher des informations sur les fichiers mis en quarantaine.

Afficher des informations sur tous les fichiers mis en quarantaine

```
kesl-control -Q --query [-n <number>] [--json]
```

Afficher des informations sur les fichiers mis en quarantaine qui correspondent aux conditions du filtre

```
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

Où :

`<filter conditions>` indique une ou plusieurs expressions logiques au format `<field> <comparison operator> '<value>'`, combinées à l'aide de l'opérateur logique `and`, afin de limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtrage, l'application affichera des informations sur tous les fichiers mis en quarantaine.

`<number>` est le nombre de fichiers les plus récemment mis en quarantaine que vous souhaitez afficher. Si vous ne spécifiez pas la clé `-n`, les 30 derniers fichiers seront affichés. Pour afficher tous les fichiers, saisissez la valeur 0.

`--json` : afficher les données au format JSON.

Commande kesl-control -Q --restore

La commande vous permet de restaurer un fichier de la quarantaine.

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

Où :

`<file ID>` est l'identifiant du fichier mis en quarantaine.

`--file <file path>` est le nouveau nom du fichier ainsi que le chemin d'accès au répertoire dans lequel l'enregistrer. Si vous ne spécifiez pas la clé `--file`, le fichier sera restauré avec son nom d'origine à son emplacement d'origine. Si le répertoire est supprimé ou si l'utilisateur n'a pas de droits d'accès à ce répertoire, l'application place le fichier dans le répertoire /var/opt/kaspersky/kesl/common/restored/. Vous pouvez déplacer manuellement le fichier de ce répertoire vers le répertoire souhaité.

Commandes d'administration du module EDR Expert (on-premises)

Le préfixe -R indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec les solutions Kaspersky Detection and Response.

Commande kesl-control --add-kataedr-server-certificate

Cette commande vous permet d'ajouter ou de remplacer un certificat précédemment ajouté pour le serveur KATA, le serveur d'actions de réponse OSMP ou le serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

Où :

`<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez ajouter ou remplacer un certificat en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous ajoutez ou remplacez un certificat de serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --remove-kataedr-server-certificate

La commande vous permet de supprimer le certificat pour le serveur KATA, le serveur d'actions de réponse OSMP ou le serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez supprimer un certificat en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous supprimez le certificat du serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --query-kataedr-server-certificate

La commande vous permet d'afficher les informations sur le certificat du serveur KATA, du serveur d'actions OSMP ou du serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez afficher les informations sur le certificat en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous souhaitez afficher des informations sur le certificat du serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --add-kataedr-client-certificate

Cette commande permet d'ajouter ou de remplacer un certificat client précédemment ajouté, utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

Où :

`<file>` est le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée.

> Vous devez spécifier le mot de passe du conteneur crypto. Sinon, lorsque vous cliquez sur **Entrée**, une erreur `Certificate password is required and cannot be empty` s'affiche.

`--server-type <response|telemetry>` permet de sélectionner le type de serveur auquel vous souhaitez ajouter un certificat client en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous ajoutez ou remplacez un certificat client pour la connexion au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control [-R] --remove-kataedr-client-certificate

Cette commande permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions de réponse OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez supprimer un certificat client en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous supprimez un certificat client utilisé pour la connexion au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control [-R] --query-kataedr-client-certificate

Cette commande affiche des informations sur le certificat client utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions de réponse OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez afficher les informations sur un certificat client en mode d'intégration EDR Expert (on-premises) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous souhaitez afficher des informations sur le certificat client utilisé pour se connecter au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commandes d'administration du module Expert EDR (cloud)

Le préfixe -R indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec les solutions Kaspersky Detection and Response.

kesl-control --query-cloudxdr-server-certificate

Cette commande permet d'afficher les informations sur le certificat du serveur d'actions de réponse OSMP ou serveur de collecte de télémétrie OSMP.

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel afficher les informations du certificat en mode d'intégration EDR Expert (cloud) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

kesl-control --query-cloudxdr-client-certificate

Cette commande permet d'afficher des informations sur un certificat client ajouté précédemment, utilisé pour sécuriser la connexion au serveur d'actions de réponse OSMP ou serveur de collecte de télémétrie OSMP.

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

Où :

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel afficher les informations sur un certificat client en mode d'intégration EDR Expert (cloud) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Commandes d'administration des modules NDR (KATA)

Le préfixe -R indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec les solutions Kaspersky Detection and Response.

Commande kesl-control --add-katandr-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat du serveur NDR précédemment ajouté.

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

Où :

`<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Commande kesl-control --remove-katandr-server-certificate

Cette commande supprime un certificat de serveur NDR.

```
kesl-control [-R] --remove-katandr-server-certificate
```

Commande kesl-control --query-katandr-server-certificate

La commande vous permet d'afficher des informations sur le certificat du serveur NDR.

```
kesl-control [-R] --query-katandr-server-certificate
```

Commande kesl-control --add-katandr-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour sécuriser la connexion au serveur NDR.

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

Où :

`<file>` est le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée.

Vous devez spécifier le mot de passe du conteneur crypto. Sinon, lorsque vous cliquez sur **Entrée**, une erreur `Certificate password is required and cannot be empty` s'affiche.

Commande kesl-control --remove-katandr-client-certificate

La commande vous permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur NDR.

```
kesl-control [-R] --remove-katandr-client-certificate
```

Commande kesl-control --query-katandr-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

```
kesl-control [-R] --query-katandr-client-certificate
```

Commandes de contrôle d'isolation réseau des appareils

Le préfixe -R indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec les solutions Kaspersky Detection and Response. L'isolement réseau des appareils est appliquée comme mesure de réponse à la détection des menaces lorsqu'elle est intégrée aux solutions Detection and Response spécifiées.

Commande kesl-control --isolation-stat

La commande permet d'afficher l'état actuel de l'isolation réseau sur la console : activée ou désactivée.

```
kesl-control [-R] --isolation-stat
```

Commande kesl-control --isolation-off

La commande vous permet de désactiver temporairement l'isolation réseau d'un appareil.

```
kesl-control [-R] --isolation-off
```

Commandes de gestion des paramètres d'intégration avec KUMA

Le préfixe -M indique que la commande appartient au groupe de commandes permettant de gérer les paramètres de Kaspersky Unified Monitoring and Analysis Platform.

Commande kesl-control --add-kuma-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat du serveur KUMA précédemment ajouté.

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

Où :

`<path to file>` correspond au chemin d'accès au fichier qui contient le certificat du serveur, au format DER ou PEM.

Commande kesl-control --remove-kuma-server-certificate

La commande permet de supprimer le certificat du serveur KUMA.

```
kesl-control [-M] --remove-kuma-server-certificate
```

Commande kesl-control --query-kuma-server-certificate

La commande vous permet d'afficher des informations sur le certificat du serveur KUMA.

```
kesl-control [-M] --query-kuma-server-certificate
```

Commande kesl-control --add-kuma-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour sécuriser la connexion au serveur KUMA.

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

Où :

`<path to file>` est le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée.

> Vous devez spécifier le mot de passe du conteneur crypto. Sinon, lorsque vous cliquez sur **Entrée**, une erreur `Certificate password is required and cannot be empty` s'affiche.

Commande kesl-control --remove-kuma-client-certificate

La commande vous permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur KATA.

```
kesl-control [-M] --remove-kuma-client-certificate
```

Commande kesl-control --query-kuma-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

```
kesl-control [-M] --query-kuma-client-certificate
```

Commandes de gestion des paramètres d'intégration avec Sandbox

Le préfixe -X indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec Sandbox.

Commande kesl-control --add-sandbox-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat précédemment ajouté du serveur qui assure l'interaction avec Sandbox.

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

Où :

`<file>` correspond au chemin d'accès au fichier qui contient le certificat du serveur, au format DER ou PEM.

kesl-control --remove-sandbox-server-certificate

La commande vous permet de supprimer le certificat du serveur qui assure la communication avec Sandbox.

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Commande kesl-control --query-sandbox-server-certificate

La commande affiche des informations sur le certificat du serveur qui permet l'interaction avec Sandbox.

```
kesl-control [-X] --query-sandbox-server-certificate
```

Commande kesl-control --add-sandbox-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour protéger la connexion au serveur qui assure l'interaction avec Sandbox.

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

Où :

`<file>` est le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée.

> Vous devez spécifier le mot de passe du conteneur crypto. Sinon, lorsque vous cliquez sur **Entrée**, une erreur `Certificate password is required and cannot be empty` s'affiche.

Commande kesl-control --remove-sandbox-client-certificate

La commande vous permet de supprimer un certificat client utilisé pour protéger la connexion au serveur qui assure l'interaction avec Sandbox.

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Commande kesl-control --query-sandbox-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

```
kesl-control [-X] --query-sandbox-client-certificate
```

Commande kesl-control --sandbox

La commande vous permet d'envoyer des fichiers à Sandbox pour analyse.

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

Où :

`<path>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

Commandes de gestion de l'analyse IOC

Le préfixe `-T` indique que la commande appartient au groupe de commandes de gestion des paramètres et des tâches de l'application.

Commande kesl-control --scan-ioc

La commande exécute une recherche d'indicateurs de compromission sur l'appareil (IOC).

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Où :

`--path <path to directory or file>` est le chemin d'accès au fichier IOC ou au répertoire contenant des fichiers IOC portant l'extension .IOC ou .XML, à utiliser pour effectuer l'analyse.

> Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces. Vous pouvez également spécifier les deux types de chemins (fichier et répertoire).

`--process` : activation de l'analyse des processus en cours d'exécution sur l'appareil.

Arguments possibles :

- `on` : activer l'analyse des processus en cours d'exécution sur l'appareil (valeur par défaut).
- `off` : désactiver l'analyse des processus en cours d'exécution sur l'appareil.

Si vous n'indiquez pas la clé `--process`, l'application effectue une analyse de processus uniquement si le fichier IOC utilisé contient les données de processus (`ProcessItem`).

`--hint <regular expression>` est l'expression régulière qui correspond au chemin complet du fichier (`FileItem`) ou du fichier exécutable du processus (`ProcessItem`) à analyser.

Vous pouvez utiliser les éléments d'expressions régulières suivants :

- métacaractères : `.` `^` `$` `|`
- classes de caractères : `digit`, `alpha`, `lower`, `upper`, `cntrl`
- quantificateurs : `*` `+` `?` `{n}` `{n,}` `{n, m}`
- négation : `[^a-c]`
- caractères d'échappement : `\a` `\e` `\f`, `\n` `\r` `\t` `\v` `\b`

`--arpentry` : activation de l'analyse des enregistrements dans la tableau ARP (`ArpEntryItem`).

Arguments possibles :

- `on` : activer l'analyse des enregistrements dans le tableau ARP (valeur par défaut).
- `off` : désactiver l'analyse des enregistrements dans le tableau ARP.

Si vous n'indiquez pas la clé `--arpentry`, l'application analyse la tableau ARP uniquement si le fichier IOC utilisé contient les données de la table (`ArpEntryItem`).

`--ports` : activation de l'analyse des ports ouverts pour la connexion.

Arguments possibles :

- `on` : activer l'analyse des ports ouverts pour les connexions et vérifier les connexions actives sur l'appareil (valeur par défaut).
- `off` : désactiver l'analyse des ports ouverts pour les connexions et ne pas vérifier les connexions actives sur l'appareil.

Si vous n'indiquez pas la clé `--ports`, l'application effectue une analyse de ports uniquement si le fichier IOC utilisé contient les données de ports (`PortItem`).

`--system` : activation de l'analyse de l'environnement système.

Arguments possibles :

- `on` : activation de l'analyse de l'environnement système (valeur par défaut).
- `off` : désactivation de l'analyse de l'environnement système.

Si vous n'indiquez pas la clé `--system`, l'application effectue une analyse de l'environnement système uniquement si les informations sur l'environnement système (`SystemInfoItem`) sont spécifiées dans le fichier IOC utilisé.

`--files` : activation de l'analyse des fichiers.

Arguments possibles :

- `on` : activation de l'analyse des fichiers (valeur par défaut).
- `off` : désactivation de l'analyse des fichiers.

Si vous n'indiquez pas la clé `--files`, l'application effectue une analyse de fichiers uniquement si le fichier IOC utilisé contient les données de fichiers (`FileItem`).

`--drives` : zones à analyser.

Arguments possibles :

- `all` : analyser toutes les zones de fichiers disponibles.
- `system` : analyser tous les fichiers du système de fichiers racine.

- `critical` : analyser les fichiers dans les répertoires utilisateur et système (valeur par défaut).
- `custom` : analyser uniquement les fichiers dans les zones que vous spécifiez.

Si vous ne spécifiez pas la clé `--drives`, l'application analyse les fichiers dans les répertoires utilisateur et système.

`--excludes <list of exclusions>` est la liste des chemins exclus de l'analyse.

Les exclusions spécifiées par cette clé sont globales et s'appliquent quel que soit le type de zone ou de liste de répertoires. Ces exclusions ont la priorité sur les autres options de ligne de commande, notamment `--hint` et `--scope`.

> Les exclusions sont spécifiées sous forme de chemins, mais ne peuvent pas contenir des éléments récursifs ni de caractères de masque (par exemple, `*`).

Si vous ne spécifiez pas la clé `--excludes`, l'analyse est effectuée sans exclusion.

Vous pouvez spécifier plusieurs exclusions, séparées par des espaces.

`--scope <list of directories>` est la liste des répertoires supplémentaires à analyser.

> Cette option est obligatoire si vous avez spécifié l'argument `--drives` pour l'option `custom`.

`--action` : action effectuée lorsque des indicateurs de compromission sont détectés.

Arguments possibles :

- `Skip` : l'application n'effectuera aucune action avec l'objet détecté, mais les informations le concernant seront enregistrées dans les résultats de la tâche (valeur par défaut).
- `QuarantineFile` : l'application mettra en quarantaine l'objet détecté.
- `IsolateHost` : l'application isole du réseau l'appareil sur lequel l'objet est détecté.
- `ScanCriticalAreas` : l'application exécutera l'analyse des zones critiques.

Zones critiques analysées par Kaspersky Endpoint Security

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart

- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Vous pouvez spécifier plusieurs actions séparées par des espaces.

> Si vous avez spécifié l'argument `Skip`, vous n'avez pas besoin d'ajouter d'autres arguments. L'argument `Skip` ne peut être utilisé que de manière indépendante.

kesl-control --get-response-task-list

Cette commande affiche des informations sur les tâches *Analyse IOC* en cours d'exécution sur l'appareil.

```
kesl-control [-T] --get-response-task-list
```

En conséquence, l'application affiche les informations sur les tâches en cours d'exécution sous la forme suivante :

Identifiant de la tâche : <ID de la tâche>

Action de réponse : locScan

Date de création : <date et heure de création de la tâche>

Début de la tâche : <planification du lancement de la tâche>

État : <état de la tâche>

Kaspersky Endpoint Security met à jour les informations sur les tâches *Analyse IOC* en cours d'exécution lors de chaque synchronisation avec le serveur. Vous pouvez configurer l'intervalle de synchronisation dans les paramètres de l'intégration avec la solution Kaspersky Detection and Response (`SynchronizationPeriod`). Par défaut, l'application se synchronise avec le serveur toutes les 5 minutes.

kesl-control --delete-response-task <task ID>

Cette commande supprime la tâche *Analyse IOC* à l'aide de son ID. L'application supprime la tâche localement sur l'ordinateur. Si vous n'avez pas supprimé la tâche dans la Web Console ou la console OSMP, l'application restaure cette tâche lors de la prochaine synchronisation avec le serveur.

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Commandes de l'application en mode Light Agent

Le préfixe -V indique que la commande appartient au groupe de commandes de Kaspersky Endpoint Security utilisées en mode Light Agent.

Les commandes peuvent être exécutées uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Commande kesl-control --ksvla-info

Cette commande affiche des informations sur l'utilisation de l'application en mode Light Agent.

```
kesl-control --ksvla-info
```

Commande kesl-control --viis-info

Cette commande affiche des informations sur l'utilisation de l'application en mode Light Agent.

```
kesl-control --viis-info
```

Commande kesl-control --svm-info

Cette commande affiche des informations sur l'utilisation de l'application en mode Light Agent.

```
kesl-control --svm-info
```

Options de ligne de commande de l'application

Tâche de mise à jour

Le tableau suivant décrit toutes les valeurs disponibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche `Update`.

Paramètres de la tâche de la mise à jour

Paramètre	Description	Valeurs
`ConnectionTimeout`	Temps d'attente (en secondes) pour une réponse de la source de mise à jour lorsque vous essayez de vous y connecter. Si la source de mise à jour n'a pas répondu à l'issue du délai indiqué, l'application contacte la source de mise à jour suivante dans la liste.	Vous pouvez indiquer uniquement des nombres entiers compris entre 0 et 120. Valeur par défaut : 10.
`ApplicationUpdateMode`	Mode de téléchargement et d'installation des mises à jour d'applications installées automatiquement (correctifs automatiques).	`Disabled` : ne pas télécharger et ne pas installer les correctifs automatiques. `DownloadOnly` (valeur par défaut) : télécharger automatiquement les correctifs automatiques, mais ne les pas installer. `DownloadAndInstall` : télécharger et installer automatiquement les correctifs automatiques. Après avoir installé le correctif automatique, l'application redémarrera automatiquement.
La section **[Sources.item_#]** contient les paramètres suivants :		
`Enabled`	Utilisation de la source de mises à jour spécifiée via le paramètre `SourceType`. Pour exécuter la tâche, il faut activer l'utilisation d'au moins une source de mise à jour.	`Yes` (valeur par défaut) : l'application utilise la source de mises à jour. `No` : l'application n'utilise pas la source de mise à jour.

Paramètre	Description	Valeurs
`SourceType`	Source à partir de laquelle l'application va recevoir les mises à jour.	`KLServers` (valeur par défaut) : l'application récupère les mises à jour depuis un des serveurs de mise à jour de Kaspersky. Les mises à jour sont téléchargées via le protocole HTTPS. `SCServer`. L'application télécharge les mises à jour sur l'appareil protégé depuis le Serveur d'administration installé dans le réseau local. Vous pouvez sélectionner cette source de mise à jour si vous utilisez l'application Kaspersky Security Center pour l'administration centralisée de la protection des appareils au sein de votre entreprise. `Custom`. L'application télécharge les mises à jour depuis une source personnalisée spécifiée dans le paramètre `URL`. Vous pouvez désigner les répertoires des serveurs HTTP, HTTP ou FTP ainsi que tous les répertoires sur tout appareil monté sur l'appareil client protégé, y compris les répertoires des appareils distants montés via les protocoles Samba ou NFS.
`URL`	Adresse de la source de mise à jour personnalisée sur le réseau local ou sur Internet.	La valeur par défaut n'est pas définie. Exemples : `URL=http://example.com/bases/` : adresse du serveur HTTP sur lequel se trouve le répertoire contenant les mises à jour. `URL=/home/bases/` : répertoire qui contient les bases de l'application sur l'appareil protégé.

Protection contre les menaces contre l'hôte

Tâche Protection contre les fichiers malicieux

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces de fichiers à l'aide de la tâche prédéfinie de protection contre les fichiers malicieux (`File_Threat_Protection`).

La tâche Protection contre les fichiers malicieux est lancée par défaut. Vous pouvez démarrer et arrêter cette tâche manuellement.

Les privilèges du rôle d'administrateur sont nécessaires pour arrêter et démarrer la tâche Protection contre les fichiers malicieux à partir de la ligne de commande.

Vous pouvez configurer les paramètres de protection contre les fichiers malicieux en modifiant les paramètres de la tâche prédéfinie Protection contre les fichiers malicieux.

Le tableau suivant décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche Protection contre les fichiers malicieux.

Paramètre	Description	Valeurs
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées. Il n'est pas recommandé d'activer ce paramètre, car l'analyse des archives réduit les performances du fait que l'accès au fichier d'archive est bloqué avant que le fichier ne soit décompressé dans un répertoire temporaire et analysé.	`Yes` : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` (valeur par défaut) : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` : analyse les archives autoextractibles. `No` (valeur par défaut) : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SkipPlainTextFiles`	Exclusion temporaire de l'analyse des fichiers au format texte. Ce paramètre permet d'optimiser l'analyse des journaux de fonctionnement des applications. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.	`Yes` : n'analyse pas les fichiers au format texte si ceux-ci ont été à nouveau utilisés par ce même processus au cours des 10 minutes suivant la dernière analyse. `No` (valeur par défaut) : analyse les fichiers au format texte.
`SkipDatabaseJournals`	Exclure temporairement les fichiers journaux de base de données de l'analyse. Ce paramètre permet d'optimiser la vérification des journaux de la base de données. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.	`Yes` : ne pas analyser les fichiers journaux de la base de données si ceux-ci ont été à nouveau utilisés par ce même processus au cours des 10 minutes suivant la dernière analyse. `No` (valeur par défaut) : analyser les fichiers journaux de la base de données.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 60.

Paramètre	Description	Valeurs
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectBlockIfNotPossible` (désinfecter ; bloquer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application bloque l'accès à l'objet infecté. `Block` (bloquer) : l'application bloque l'accès à un objet infecté. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque.
	Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
		La valeur par défaut n'est pas définie.
		`Exemple`
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		`Exemple`
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.

Paramètre	Description	Valeurs
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`ScanByAccessType`	Mode de fonctionnement de la tâche Protection contre les fichiers malicieux. Le paramètre `ScanByAccessType` s'applique seulement à la tâche de protection contre les fichiers malicieux.	`SmartCheck` (valeur par défaut) : analyse un fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture s'il a été modifié. Si un processus lors de son fonctionnement accède plusieurs fois à un fichier et le modifie, l'application analyse à nouveau le fichier uniquement lorsque le processus le ferme pour la dernière fois. `OpenAndModify` : analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture s'il a été modifié. `Open` : analyse le fichier en cas de tentative d'ouverture en lecture, ou pour exécution ou modification.
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`. Exemple `AreaDesc="Scanning of email databases"`
`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple `AreaMask_item_<item number>=*doc`

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<path to local folder>` – Analyser les objets dans le répertoire indiqué. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application évite d'analyser uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut de l'analyse tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets de l'analyse).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local folder>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des masques et des tags pour spécifier le chemin. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedForProgram.item_#]** contient les paramètres suivants :		
`ProgramPath`	Chemin d'accès au processus exclu. Si un module de noyau mis à jour est utilisé pour intercepter les événements système, le processus spécifié est exclu de l'interception dans tous les espaces de noms.	`<path to process>` — Exclure de l'analyse les objets du répertoire indiqué.
`ApplyToDescendants`	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre `ProgramPath`.	`Yes` : exclut le processus spécifié et tous ses processus enfants de l'analyse. `No` (valeur par défaut) : exclut uniquement le processus spécifié de l'analyse, n'exclut pas les processus enfants de l'analyse.

Paramètre	Description	Valeurs
`AreaDesc`	Description de la zone d'exclusion de processus.	Valeur par défaut : `All objects`.
`UseExcludedForProgram`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de processus. Dans la zone d'exclusion des processus, l'application évite d'analyser uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut de l'analyse tous les objets de la zone d'exclusion des processus. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets de l'analyse).
`Path`	Chemin d'accès au répertoire contenant des fichiers que le processus modifie.	`<path to local folder>` — Exclure de l'analyse les objets du répertoire indiqué. Vous pouvez utiliser des masques pour spécifier le chemin. `Shared:NFS` : exclut de l'analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : exclut de l'analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : exclut de l'analyse toutes les ressources du système de fichiers de l'appareil partagées via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Optimisation de la vérification des répertoires réseau

Pour optimiser la protection contre les menaces de fichiers, vous pouvez configurer l'exclusion de l'analyse des fichiers copiés des répertoires réseau vers un répertoire local. Pour ce faire, vous devez configurer une exclusion de processus pour un utilitaire conçu pour copier à partir de répertoires réseau (par exemple, pour l'utilitaire `cp`).

Pour configurer l'exclusion des répertoires réseau de l'analyse :

1. Exportez les paramètres de la tâche Protection contre les fichiers malicieux (`File_Threat_Protection`, ID:1) dans un fichier de configuration à l'aide de la commande suivante :

   ```
   kesl-control --get-settings 1 --file <full path to the configuration file> [--json]
   ```

2. Ouvrez le fichier de configuration et ajoutez une section `[ExcludedForProgram.item_#]` avec les paramètres suivants :

   - `ProgramPath` : chemin d'accès au processus à exclure ou au répertoire contenant des processus à exclure.
   - `ApplyToDescendants` – paramètre indiquant si les processus enfants du processus exclu doivent être exclus de l'analyse (valeurs possibles : `Yes` ou `No`).
   - `AreaDesc` : description de la zone d'exclusion en fonction des processus et qui contient des informations supplémentaires sur la zone d'exclusion.
   - `UseExcludedForProgram` : activer l'exclusion de la zone spécifiée lorsque la tâche est en cours d'exécution (valeurs possibles : `Yes` ou `No`).
   - `Path` : chemin d'accès au répertoire contenant des fichiers que le processus modifie.
   - `AreaMask.item_#` : masque de nom de fichier pour les fichiers à exclure de l'analyse. Vous pouvez également renseigner le chemin d'accès complet au fichier.

   Exemple

   ```
   [ExcludedForProgram.item_0000]
   ProgramPath=/usr/bin/cp
   ApplyToDescendants=No
   AreaDesc=
   UseExcludedForProgram=Yes
   Path=AllRemoteMounted
   AreaMask.item_0000=*
   ```

3. Exécutez la commande:

   ```
   kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
   ```

   Spécifiez la clé `--json` si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

L'application n'analysera pas les fichiers dans les répertoires réseau, mais la commande `cp` (pour l'exemple cité ci-dessus) et les fichiers locaux seront quant à eux vérifiés.

Analyse des logiciels malveillants

À partir de la ligne de commande, vous pouvez analyser des logiciels malveillants des manières suivantes :

- Utilisation de la tâche prédéfinie Analyse des logiciels malveillants (`Scan_My_Computer`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.
- Utilisation de tâches personnalisées d'analyse des logiciels malveillants (tâches de type `ODS`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche.

Vous pouvez effectuer une *analyse personnalisée* des fichiers et des répertoires indiqués à l'aide de la commande suivante :

```
kesl-control --scan-file
```

Tâche d'analyse des logiciels malveillants

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Analyse des logiciels malveillants (`Scan_My_Computer`).

Paramètres d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fichiers. `No` : ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.

Paramètre	Description	Valeurs
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

Paramètre	Description	Valeurs
`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `<device name mask>` – Analyser les secteurs d'amorçage des appareils dont le nom correspond au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		

`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
		`Exemple`
		`AreaDesc="Mail bases scan"`

`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.

Paramètre	Description	Valeurs

`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell.
	Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.
		Valeur par défaut : `*` (analyser tous les objets).
		`Exemple`
		`AreaMask.item_0000=*doc`

`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<path to local directory>` – Analyser les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des masques pour spécifier le chemin. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Tâche d'analyse personnalisée

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche d'analyse personnalisée (`Scan_File`).

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fichiers. `No` : ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` : analyser les secteurs d'amorçage. `No` (valeur par défaut) — ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` — analyser la mémoire des processus et la mémoire du noyau. `No` (valeur par défaut) : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` : analyser les objets de démarrage. `No` (valeur par défaut) — ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.

Paramètre	Description	Valeurs
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) pour ne pas exclure de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.	La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) pour utiliser les exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) pour utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.

Paramètre	Description	Valeurs
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) pour ne pas enregistrer dans le journal les informations relatives aux objets non infectés.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) pour ne pas enregistrer dans le journal les informations relatives aux objets analysés dans les archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) pour ne pas enregistrer dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) pour activer l'analyse heuristique. `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) – Valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) pour activer l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `<device name mask>` – Analyser les secteurs d'amorçage des appareils dont le nom correspond au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).

Tâche d'analyse des zones critiques

Le tableau ci-dessous décrit toutes les valeurs disponibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Analyse des zones critiques (`Critical_Areas_Scan`).

Paramètres de la tâche d'analyse des zones critiques

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` : analyse les fichiers. `No` (valeur par défaut) — Ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.

Paramètre	Description	Valeurs
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.

Paramètre	Description	Valeurs
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.

Paramètre	Description	Valeurs
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `<device name mask>` – Analyser les secteurs d'amorçage des appareils dont le nom correspond au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		

`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
		`Exemple`
		`AreaDesc="Mail bases scan"`

`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.

`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell.
	Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.
		Valeur par défaut : `*` (analyser tous les objets).
		`Exemple`
		`AreaMask.item_0000=*doc`

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<path to local directory>` – Analyser les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des masques pour spécifier le chemin. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Tâche d'analyse des disques amovibles

Sur la ligne de commande, vous pouvez gérer l'analyse des disques amovibles à l'aide de la tâche prédéfinie Analyse des disques amovibles (`Removable_Drives_Scan`).

Par défaut, la tâche *Analyse des disques amovibles* n'est pas démarrée. Vous pouvez démarrer et arrêter cette tâche manuellement. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

Si la tâche est en cours d'exécution, l'application surveille la connexion des disques amovibles à l'appareil et, lorsqu'un disque amovible est connecté, crée et exécute une tâche temporaire d'analyse du secteur de démarrage (tâche de type `ODS`). Cette tâche ne peut pas être arrêtée. Une fois la tâche exécutée, l'application la supprime automatiquement.

Si vous avez activé l'analyse des fichiers dans les paramètres de la tâche *Analyse des disques amovibles*, l'application exécute également une ou plusieurs tâches temporaires d'analyse personnalisée des fichiers (tâches de type `ODS`). Si nécessaire, un utilisateur disposant de privilèges d'administrateur peut arrêter l'exécution de telles tâches.

Lors de la modification des paramètres de la tâche *Analyse des disques amovibles*, les nouvelles valeurs ne sont pas appliquées aux tâches temporaires déjà en cours d'exécution. Lorsque vous arrêtez la tâche *Analyse des disques amovibles*, les tâches temporaires déjà en cours d'exécution ne sont pas arrêtées.

Paramètres de tâche d'analyse des disques amovibles

Paramètre	Description	Valeurs
`ScanRemovableDrives`	Activation de l'analyse des disques amovibles lors de la connexion à l'appareil. Cette option n'est pas appliquée aux lecteurs CD/DVD et aux disques Blu-ray (cf. le paramètre `ScanOpticalDrives`).	`DetailedScan`. Analyser tous les fichiers sur les supports amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray). Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche `Scan_File` (ID:3). `QuickScan`. Analyser uniquement les fichiers de **certains types** sur les supports amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray). Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. L'analyse rapide est effectuée avec les paramètres par défaut de la tâche `Critical_Areas_Scan` (ID:4). `NoScan` (valeur par défaut) : n'analyse pas les disques amovibles lors de la connexion.

Paramètre	Description	Valeurs
`ScanOpticalDrives`	Activation de l'analyse des lecteurs CD/DVD et des disques Blu-ray lors de la connexion à l'appareil.	`DetailedScan`. Analyser tous les fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche `Scan_File` (ID:3). `QuickScan`. Analyser uniquement les fichiers de **certains types** sur les lecteurs CD/DVD et les disques Blu-ray. Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. L'analyse rapide est effectuée avec les paramètres par défaut de la tâche `Critical_Areas_Scan` (ID:4). `NoScan` (valeur par défaut). Ne pas analyser les lecteurs CD/DVD et les disques Blu-ray à leur connexion.
`BlockDuringScan`	Activation du blocage des fichiers à la connexion du disque lors de l'analyse. Lors de l'analyse des secteurs de démarrage, les fichiers ne sont pas bloqués.	`Yes` : bloque les fichiers pendant l'analyse. `No` (valeur par défaut) : ne bloque pas les fichiers pendant l'analyse.

Analyser les conteneurs

À partir de la ligne de commande, vous pouvez analyser les conteneurs et les images des manières suivantes :

- Utilisation de la tâche prédéfinie Analyse du conteneur (`Container_Scan`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

- Utilisation des tâches définies par l'utilisateur de l'Analyse du conteneur (tâches de type `ContainerScan`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche.

- À l'aide de la commande suivante, vous pouvez effectuer une *analyse personnalisée* des conteneurs et des images spécifiés :

  ```
  kesl-control --scan-container
  ```

Paramètres d'analyse de conteneur

Le tableau suivant décrit les paramètres de l'analyse du conteneur utilisés lors de l'analyse en temps réel des espaces de noms et des conteneurs.

Paramètres généraux d'analyse du conteneur et des espaces de noms

Paramètre	Description	Valeurs
`OnAccessContainerScanAction`	Spécifie l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté. Cette option est disponible lors de l'utilisation de l'application sous une licence qui active cette fonctionnalité. Lors de l'analyse des objets à l'intérieur d'un conteneur, les paramètres de la tâche Protection contre les fichiers malicieux sont utilisés.	`StopContainerIfFailed` (valeur par défaut) : arrête le conteneur en cas d'échec de la désinfection ou de la suppression d'un objet infecté. Si cette valeur est sélectionnée, l'action effectuée sur le conteneur dépend également de la valeur spécifiée du paramètre `ActionOnThreat` de la tâche Protection contre les fichiers malicieux. Si le paramètre `ActionOnThreat` est défini sur `DisinfectDeleteIfNotPossible` et que l'application ne parvient pas à désinfecter ou à supprimer l'objet infecté lors de l'exécution de l'action, le conteneur sera arrêté. `StopContainer` : arrête le conteneur à la suite de la détection d'un objet infecté. `Skip` : n'effectue aucune action sur les conteneurs lorsqu'un objet infecté a été détecté.
`UseDocker`	Utilisation du système d'administration par les conteneurs Docker.	`Yes` (valeur par défaut) : utiliser le système d'administration par les conteneurs Docker. `No` : ne pas utiliser le système d'administration par les conteneurs Docker.
`DockerSocket`	Chemin ou URI (ID universel de ressource) du socket de Docker.	Valeur par défaut : /var/run/docker.sock.
`UseCrio`	Utilisation de l'environnement CRI-O.	`Yes` (valeur par défaut) : utilise l'environnement CRI-O. `No` : n'utilise pas l'environnement CRI-O.
`CrioConfigFilePath`	Chemin d'accès au fichier de configuration CRI-O.	Valeur par défaut : /etc/crio/crio.conf.
`UsePodman`	Utilisation de l'utilitaire Podman.	`Yes` (valeur par défaut) : utilise l'utilitaire Podman. `No` : n'utilise pas l'utilitaire Podman.
`PodmanBinaryPath`	Chemin d'accès au fichier exécutable de l'utilitaire Podman.	Valeur par défaut : /usr/bin/podman.
`PodmanRootFolder`	Chemin de la racine du stockage de conteneurs.	Valeur par défaut : /var/lib/containers/storage.
`UseRunc`	Utilisation de l'utilitaire runc.	`Yes` (valeur par défaut) : utilise l'utilitaire runc. `No` : n'utilise pas l'utilitaire runc.
`RuncBinaryPath`	Chemin d'accès au fichier exécutable de l'utilitaire runc.	Valeur par défaut : /usr/bin/runc.
`RuncRootFolder`	Chemin de la racine du Stockage des états de conteneurs.	Valeur par défaut : /run/runc.

Tâche Analyse du conteneur

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche Analyse du conteneur (`Container_Scan`).

Paramètre	Description	Valeurs
`ScanContainers`	Analyse des conteneurs spécifiés par un masque Vous pouvez définir les masques à l'aide du paramètre `ContainerNameMask`.	`Yes` (valeur par défaut) : analyse les conteneurs définis par masque. `No` : n'analyse pas les conteneurs définis par masque.

`ContainerNameMask`	Nom ou un masque de nom qui définit un conteneur à analyser.
	Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères ? et *.
	Avant de définir ce paramètre, assurez-vous que la valeur du paramètre `ScanContainers=Yes`.
		Valeur par défaut : * (analyser tous les conteneurs).
		`Exemple d'analyse d'un conteneur effectuée sur un conteneur nommé my_container`
		`ContainerNameMask=my_container`
		`Exemple d'analyse de tous les conteneurs dont les noms commencent par my_container`
		`ContainerNameMask=my_container*`
		`Exemple d'analyse de conteneur effectuée sur tous les conteneurs dont les noms commencent par my_, puis contiennent cinq caractères quelconques, puis _container et se terminent par une séquence quelconque de caractères`
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Analyse des images spécifiées par un masque Vous pouvez définir les masques à l'aide du paramètre `ImageNameMask`.	`Yes` (valeur par défaut) : analyse les images définies par masque. `No` : n'analyse pas les images définies par masque.

`ImageNameMask`	Spécifie un nom ou un masque de nom qui définit les images à analyser.
	Avant de définir ce paramètre, assurez-vous que le paramètre `ScanImages` possède la valeur `Yes`.
	Les masques sont définis dans le format de l'interpréteur de commandes.
	Si vous souhaitez définir plusieurs masques, chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.
		Valeur par défaut : * (analyser tous les modèles).
		`Exemple d'analyse d'images effectuée sur des images portant le nom "my_image" et le tag "latest"`
		`ImageNameMask=my_image:latest`
		`Exemple d'analyse d'images effectuée sur toutes les images dont les noms commencent par my_image_ et avec n'importe quel tag`
		`ImageNameMask=my_image*`

`DeepScan`	Analyse de toutes les couches des images et des conteneurs lancés.	`Yes` : analyse toutes les couches. `No` (valeur par défaut) : n'analyse pas toutes les couches.
`ContainerScanAction`	Spécifie l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté. Les actions sur un objet infecté à l'intérieur du conteneur sont décrites ci-dessous.	`StopContainerIfFailed` (valeur par défaut) : l'application arrête le conteneur si elle ne parvient pas à désinfecter ou à supprimer l'objet infecté. Lorsque cette valeur est sélectionnée, l'action effectuée sur le conteneur dépend également de la valeur spécifiée du paramètre `ActionOnThreat`, qui s'applique aux objets à l'intérieur des conteneurs et des images (voir le tableau ci-dessous). Si le paramètre `ActionOnThreat` est défini sur `DisinfectDeleteIfNotPossible` et que l'application ne parvient pas à désinfecter ou à supprimer l'objet infecté lors de l'exécution de l'action, le conteneur sera arrêté. En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action `StopContainer`. `StopContainer` : l'application arrête le conteneur lorsqu'un objet infecté est détecté. `Skip` : l'application n'effectue aucune action sur les conteneurs lorsqu'un objet infecté est détecté.
`ImageAction`	Spécifie l'action à effectuer sur une image lorsqu'un objet infecté est détecté. Les actions sur un objet infecté à l'intérieur de l'image sont décrites ci-dessous.	`Skip` (valeur par défaut) : l'application n'effectue aucune action sur l'image lorsqu'un objet infecté est détecté. `Delete` : l'application supprime l'image lorsqu'un objet infecté est détecté (non recommandé). Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.

Les paramètres décrits ci-dessous sont appliqués aux objets à l'intérieur des conteneurs et des images.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description	Valeurs
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Utilisation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.	La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

Paramètre	Description	Valeurs
`UseExcludeThreats`	Utilisation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.

Paramètre	Description	Valeurs
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`QueueScanTasks`	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, l'exécution d'une tâche d'analyse est planifiée à 18 h 00 et à 20 h 00. La tâche d'analyse dont l'exécution est planifiée à 20 h 00 est retardée si l'analyse de 18 h 00 est toujours en cours. La tâche retardée est exécutée une fois la tâche de 18 h 00 terminée.	`Yes` pour mettre en file d'attente les tâches d'analyse planifiées si l'analyse en cours n'est pas terminée. `No` (valeur par défaut) pour exécuter les tâches d'analyse planifiées même si l'analyse en cours n'est pas terminée.

Intégration à Jenkins

Kaspersky Endpoint Security prend en charge l'intégration à Jenkins. Les plug-ins Jenkins Pipeline peuvent être utilisés pour analyser des images Docker à différentes étapes. Par exemple, vous pouvez analyser des images Docker dans un référentiel pendant le processus de développement ou avant la publication.

Pour intégrer Kaspersky Endpoint Security à Jenkins :

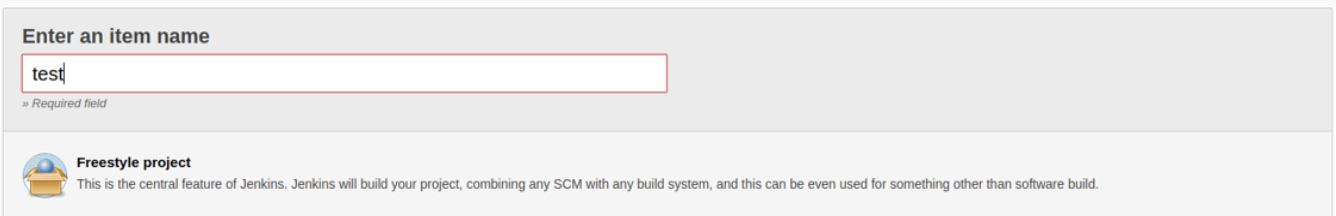
1. Installez Kaspersky Endpoint Security sur un nœud Jenkins.
2. Installez Docker Engine sur un nœud Jenkins.

   Pour en savoir plus, reportez-vous à la documentation de Docker Engine.
3. Octroyez les privilèges d'administrateur de Kaspersky Endpoint Security à l'utilisateur Jenkins :

   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```
4. Ajoutez un utilisateur Jenkins au groupe docker :

   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

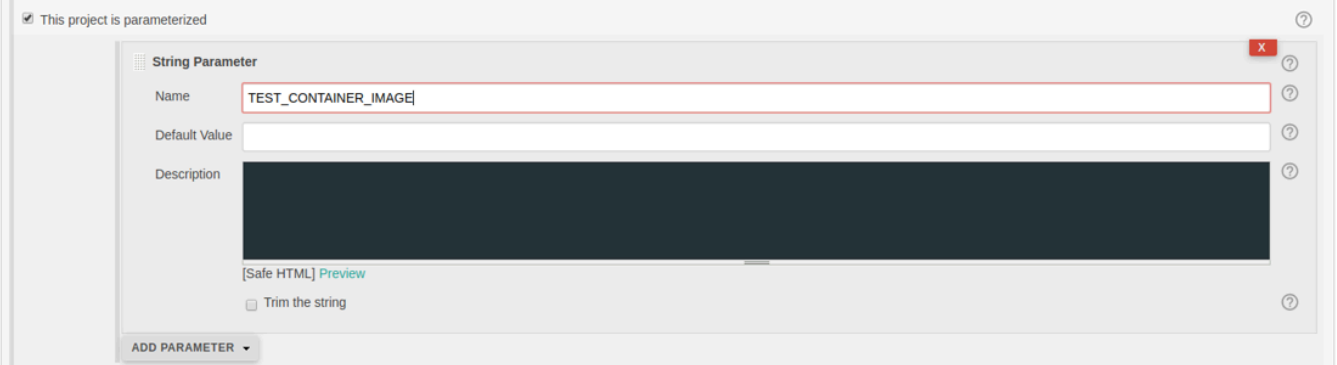
   En général, le nom jenkins est utilisé.
5. Dans Jenkins, créez une tâche de compilation nommée `test` (**New Item** → **Enter an item name**).

6. Configurez votre projet, selon vos besoins. On suppose qu'en conséquence, vous avez une image ou un conteneur démarré que vous devez analyser.

7. Pour démarrer le conteneur Docker, ajoutez le script suivant à la procédure de build Jenkins. Si vous utilisez des plug-ins Jenkins ou un autre moyen de démarrer des conteneurs Docker, enregistrez l'ID du conteneur Docker en cours d'exécution dans le fichier /tmp/kesl_cs_info en vue d'une analyse ultérieure :

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. Après avoir construit les artefacts, ajoutez le script suivant aux étapes de construction des jenkins.

   Ce script prend en charge un conteneur pour l'analyse. Si nécessaire, modifiez le script selon vos besoins.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Pour analyser une image Docker à partir d'un référentiel, utilisez le script suivant :

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Enregistrez la tâche de build.

Tâche Protection contre le chiffrement

Depuis la ligne de commande, vous pouvez gérer la protection contre le chiffrement à l'aide de la tâche Protection contre le chiffrement (`Anti_Cryptor`).

Par défaut, la tâche Protection contre le chiffrement n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres de protection contre le chiffrement en modifiant les paramètres de la tâche prédéfinie de protection contre le chiffrement.

Paramètres de la tache de Protection contre le chiffrement

Paramètre	Description	Valeurs
`ActionOnDetect`	Active les blocages des appareils douteux.	`Block` (valeur par défaut) : active le blocage des hôtes douteux. `Notify` : désactiver le blocage des appareils douteux.
`BlockTime`	Durée de blocage d'un appareil non fiable en minutes. Si un appareil compromis est bloqué et si vous modifiez la valeur du paramètre `BlockTime`, la durée de blocage de cet appareil ne change pas. La durée de blocage n'est pas une valeur dynamique et se calcule au moment du blocage.	Entier entre 1 et 4294967295. Valeur par défaut : 30.
`UseExcludeMasks`	Active l'exclusion, de la zone de protection, des objets définis à l'aide du paramètre `ExcludeMasks.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de protection les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de protection les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion, de la zone de protection, des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone de protection indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Si vous souhaitez définir plusieurs masques, indiquez chaque masque sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.

Paramètre	Description	Valeurs
La section **[ScanScope.item_#]** contient les zones protégées par l'application. Pour la tâche Protection contre le chiffrement, il faut indiquer au moins une zone de protection. Seuls les répertoires partagés peuvent être indiqués. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de protection contient des informations complémentaires sur la zone de protection.	Valeur par défaut : `All shared directories`.
`UseScanArea`	Active la protection de la zone définie. Pour exécuter la tâche, il faut inclure au moins une zone de protection.	`Yes` (valeur par défaut) : protège la zone définie. `No` : ne protège pas une zone définie.
`AreaMask.item_#`	Restriction de la zone de protection. Dans la zone de protection, l'application protège uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (protéger tous les objets).
`Path`	Chemin d'accès au répertoire contenant les objets protégés.	`< chemin d'accès au répertoire local >` – Protéger un répertoire local accessible via SMB/NFS. Vous pouvez utiliser des masques pour spécifier le chemin. `AllShared` (valeur par défaut) : protège toutes les ressources partagées via SMB/NFS. `Shared:SMB` – Protéger les ressources accessibles via SMB. `Shared:NFS` – Protéger les ressources accessibles via NFS.
La section **[ExcludedFromScanScope.item_#]** contient les objets à exclure de toutes les sections [ScanScope.item_#]. Les objets qui satisfont aux règles de n'importe quelle section [ExcludedFromScanScope.item_#] ne sont pas analysés. Le format d'une section [ExcludedFromScanScope.item_#] est identique au format d'une section [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de la protection contient des informations complémentaires sur la zone d'exclusion.	Valeur par défaut : `All objects`.
`UseScanArea`	Exclusion de la zone de protection indiquée.	`Yes` (valeur par défaut) : exclut une zone définie de la protection. `No` : n'exclut pas la zone définie de la protection.
`AreaMask.item_#`	Restriction de la zone d'exclusion de la protection. Dans la zone d'exclusion, l'application exclut uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets).
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la protection.	`< chemin d'accès au répertoire local >` – Exclure de la protection les objets du répertoire indiqué. Vous pouvez utiliser des masques pour spécifier le chemin. `Mounted:NFS` : exclure de la protection les répertoires distants montés sur l'appareil client via le protocole NFS. `Mounted:SMB` : exclure de la protection les répertoires distants montés sur l'appareil client via le protocole Samba. `AllRemoteMounted` : exclut de la protection tous les répertoires distants montés sur l'appareil distant via les protocoles Samba et NFS.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Tâche Détection comportementale

Vous pouvez gérer la Détection comportementale des applications dans le système d'exploitation en ligne de commande à l'aide de la tâche prédéfinie de Détection comportementale (`Behavior_Detection`).

La tâche Détection comportementale est exécutée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la détection comportementale en modifiant les paramètres de la tâche prédéfinie Détection comportementale.

Paramètres de la tâche Détection comportementale

Paramètre	Description	Valeurs
`UseTrustedPrograms`	Exclusion de processus de l'analyse.	`Yes` : exclut l'activité des processus spécifiés de l'analyse. `No` (valeur par défaut) : analyse tous les processus.
`TaskMode`	Action exécutée par l'application suite à la détection d'une activité malveillante dans le système d'exploitation.	`Block` (valeur par défaut) : termine le processus de l'application qui exécute une activité malveillante. `Notify` : ne met pas fin au processus qui exécute une activité malveillante, consigne uniquement la détection d'une activité malveillante dans le journal des événements.

Paramètre	Description	Valeurs
TelemetrySource	Paramètres avancés de collecte de télémétrie envoyés aux solutions Detection and Response lors de l'intégration avec ces solutions. Le paramètre `UseTelemetryMonopolyMode` est appliqué uniquement si le paramètre `TelemetrySource` est défini sur `Default`.	`Default` (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie. `OnlyEBPF` : utiliser uniquement la technologie eBPF pour la collecte de télémétrie.
UseTelemetryMonopolyMode	Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`True` (valeur par défaut) : Kaspersky Endpoint Security utilise le service auditd en mode exclusif. `False` signifie que le service auditd est utilisé en mode multidiffusion.
La section **[TrustedPrograms.item_#]** contient les processus exclus de l'analyse par le module Détection comportementale. Kaspersky Endpoint Security ne contrôle pas l'activité des processus renseignés.		
`ProgramPath`	Chemin d'accès au processus exclu.	`< chemin d'accès complet au processus >` – Exclut de l'analyse le processus dans le répertoire local spécifié. Vous pouvez utiliser des masques pour spécifier le chemin.
`ApplyToDescendants`	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre `ProgramPath`.	`Yes` : exclut le processus spécifié et tous ses processus enfants de l'analyse. `No` (valeur par défaut) : exclut uniquement le processus spécifié de l'analyse, n'exclut pas les processus enfants de l'analyse.
`ProgramDesc`	Description du processus exclu.	
`UseTrustedProgram`	Utilisation de l'exclusion de l'activité du processus spécifié de l'analyse.	`Yes` (valeur par défaut) : utiliser une exclusion de l'analyse d'activité pour le processus spécifié. `No` : ne pas utiliser l'exclusion de l'activité du processus spécifié de l'analyse.
`UseTrustedProgramForDetects`	Exclusion de l'analyse de l'activité du processus lors de l'exécution du module Détection comportementale.	`Yes` : exclure de l'analyse l'activité du processus spécifié lors de l'exécution du module Détection comportementale. `No` (valeur par défaut) : ne pas exclure de l'analyse l'activité du processus spécifié lorsque le module Détection comportementale est en cours d'exécution.
`UseTrustedProgramForMDRAndEDR`	Exclusion de l'activité de processus de la télémétrie collectée par les modules MDR et EDR Expert (on-premises). Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : exclure l'activité de ce processus de la télémétrie collectée par les modules MDR et EDR Expert (on-premises). `No` (valeur par défaut) : ne pas exclure l'activité du processus spécifié de la télémétrie.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Protection contre les Exploits

En ligne de commande, vous pouvez gérer la Protection contre les Exploits à l'aide des paramètres de la tâche prédéfinie Détection comportementale (`Behavior_Detection`).

Vous pouvez configurer les paramètres de la protection contre les Exploits, en modifiant les paramètres de la tâche prédéfinie Détection comportementale (cf. tableau ci-dessous).

Paramètres de protection contre les exploits

Paramètre	Description	Valeurs
`UseAEP`	Activation du module Protection contre les Exploits.	`Yes` active la Protection contre les Exploits. `No` (valeur par défaut) : désactiver la Protection contre les Exploits.
`AEPMode`	L'action exécutée par l'application lorsqu'elle détecte un Exploit.	`Block` (valeur par défaut) : bloquer les actions malveillantes de l'Exploit et enregistre les informations à ce sujet dans le journal des événements. `Notify` : ne pas bloquer les actions d'exploit, mais enregistrer uniquement les informations sur la détection d'exploit dans le journal des événements.
La section **[AEPExclusions.item_#]** contient les exclusions d'analyse effectuées par le module Protection contre les Exploits.		
`Enabled`	Activation d'utilisation d'une exclusion d'analyse par le module Protection contre les Exploits.	`Yes` (valeur par défaut) – utiliser l'exclusion de la Protection contre les Exploits. `No` : ne pas utiliser l'exclusion d'analyse par Protection contre les Exploits.
`DetectName`	Exclusion d'un objet de l'analyse en fonction du nom de la menace détectée dans cet objet. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseDetectName` est activé.	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet. Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
`Hash`	Exclusion d'analyse du fichier dans lequel une menace a été détectée, en fonction de son hachage. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseHash` est activé.	
`HashType`	Type de somme de hachage du fichier à exclure de l'analyse à l'aide du paramètre `Hash`.	`Md5` : type de somme de hachage MD5. `Sha256` : type de somme de hachage SHA256.
`Path`	Exclusion d'analyse d'un fichier dans lequel une menace a été détectée, ainsi que le long du chemin d'accès à ce fichier. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UsePath` est activé.	`< chemin d'accès complet au fichier ou au répertoire local >` – exclure le fichier ou les objets du répertoire spécifié (y compris les sous-répertoires) des analyses. Vous pouvez utiliser des symboles `*` et `?` pour spécifier le chemin.
`UseDetectName`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `DetectName`.	`Yes` (valeur par défaut) : exclure de l'analyse les objets contenant les menaces désignées par le paramètre `DetectName`. `No` : ne pas exclure de l'analyse les objets contenant les menaces définies par le paramètre `DetectName`.

Paramètre	Description	Valeurs
`UseHash`	Activation de l'exclusion d'analyse du fichier dans lequel une menace a été détectée, en fonction de sa somme de hachage. La somme de hachage du fichier est spécifié à l'aide du paramètre `Hash`.	`Yes` (valeur par défaut) : exclure de l'analyse le fichier contenant la menace détectée, en fonction de sa valeur de la somme de hachage. `No` : ne pas exclure de l'analyse le fichier contenant la menace détectée, en fonction de sa valeur de la somme de hachage.
`UsePath`	Activation de l'exclusion d'analyse du fichier contenant la menace détectée, en fonction de son chemin d'accès. Le chemin d'accès est spécifié à l'aide du paramètre `Path`.	`Yes` (valeur par défaut) : exclure de l'analyse le fichier dans lequel la menace a été détectée sur le chemin d'accès. `No` : ne pas exclure de l'analyse le fichier dans lequel la menace a été détectée sur le chemin d'accès.

Utilisation de Kaspersky Security Network

Depuis la ligne de commande, vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide de l'option `UseKSN` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre `UseKSN` à l'aide d'options de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Pour activer l'utilisation de Kaspersky Security Network à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

où :

`<Extended/Basic>` : mode Kaspersky Security Network.

`--accept-ksn` : option signifiant que vous acceptez les conditions de la Déclaration de Kaspersky Security Network. Vous confirmez avoir entièrement lu, compris et accepté les termes de la Déclaration de Kaspersky Security Network.

Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire /opt/kaspersky/kesl/doc/.

Pour désactiver l'utilisation de Kaspersky Security Network à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=No
```

Pour activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide du fichier de configuration, exécutez la commande suivante :

```
kesl-control --set-app-settings --file <path to the configuration file> [--json] [--accept-ksn]
```

où :

`--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux de l'application, dans lequel est configurée la valeur requise du paramètre `UseKSN`.

`--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

`--accept-ksn` : option signifiant que vous acceptez les conditions de la Déclaration de Kaspersky Security Network. La clé est requise si vous activez l'utilisation de Kaspersky Security Network.

Si Kaspersky Endpoint Security, installé sur un appareil client, fonctionne sous une stratégie de Kaspersky Security Center, la valeur du paramètre `UseKSN` peut être modifiée uniquement à l'aide de Kaspersky Security Center. Quand l'application Kaspersky Endpoint Security, installée sur un appareil client, n'est plus soumis à la stratégie, la valeur du paramètre devient `UseKSN=No`.

Connexion à Kaspersky Security Network

Pour vérifier la connexion à Kaspersky Security Network, exécutez la commande suivante :

```
kesl-control --app-info
```

La ligne **Utilisation de Kaspersky Security Network** affiche l'état de la connexion à Kaspersky Security Network :

- Si l'état *Mode étendu de KSN* est affiché, l'application Kaspersky Endpoint Security utilise Kaspersky Security Network, des informations peuvent être obtenues dans la base de connaissances, et des statistiques anonymes et des informations sur les types et les sources des menaces sont envoyées.
- Si l'état *Mode KSN de base* est affiché, l'application Kaspersky Endpoint Security utilise Kaspersky Security Network et des informations peuvent être obtenues dans la base de connaissances, mais les statistiques anonymes et les informations sur les types et les sources des menaces ne sont pas envoyées.
- Si l'état *KSN n'est pas utilisé* est affiché, l'application Kaspersky Endpoint Security n'utilise pas Kaspersky Security Network.

La ligne **Infrastructure de Kaspersky Security Network** affiche des informations sur la solution d'infrastructure utilisée pour travailler avec les bases de données de réputation de Kaspersky : *KSN* ou *KPSN*.

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- l'appareil de l'utilisateur n'est pas connecté à Internet.
- L'utilisation du Kaspersky Security Network est désactivée.
- L'application n'est pas activée ou la licence a expiré.
- Des problèmes liés à la clé de licence ont été détectés. Par exemple, la clé figure dans la liste des clés interdites.

Activation ou désactivation du mode Cloud

Le *mode Cloud* est le mode de fonctionnement de l'application Kaspersky Endpoint Security, qui utilise une version allégée des bases de données des logiciels malveillants.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation de bases de données de logiciels malveillants légers n'est pas prise en charge. L'application reçoit du Serveur de protection les bases de données spéciales nécessaires au fonctionnement du Light Agent.

À partir de la ligne de commande, vous pouvez activer et désactiver le mode cloud à l'aide du paramètre `CloudMode=Yes/No` dans les paramètres généraux de l'application.

Vous pouvez modifier le paramètre `CloudMode` à l'aide d'un fichier de configuration qui contient tous les paramètres généraux de l'application, ou à l'aide d'options de ligne de commande.

Le mode cloud de l'application est disponible si l'utilisation de Kaspersky Security Network est activée.

Tâche Protection BadUSB

À partir de la ligne de commande, vous pouvez gérer la protection BadUSB à l'aide de la tâche prédéfinie Protection BadUSB (`Bad_USB`).

La tâche Protection BadUSB n'est pas lancée par défaut. Vous pouvez démarrer et arrêter cette tâche manuellement.

Les privilèges du rôle Administrateur sont nécessaires pour arrêter et démarrer la tâche Protection BadUSB à partir de la ligne de commande.

Vous pouvez configurer les paramètres de la Protection BadUSB en modifiant les paramètres de la tâche prédéfinie Protection BadUSB.

Le tableau ci-dessous décrit les valeurs disponibles et les valeurs par défaut pour les paramètres que vous pouvez définir pour la tâche Protection BadUSB.

Paramètres de la tâche Protection BadUSB

Paramètre	Description	Valeurs
`MaxAuthAttempts`	Le nombre maximal de tentatives d'authentification de l'appareil USB après lesquelles l'application bloque l'appareil USB et toutes les tentatives d'authentification suivantes pendant la durée spécifiée par le paramètre `TimeoutAfterAttempts`.	Valeurs possibles : 1 à 10. Valeur par défaut : 5.
`TimeoutAfterAttempts`	La durée de verrouillage de l'appareil USB après le nombre de tentatives infructueuses de saisie du code d'autorisation défini par le paramètre `MaxAuthAttempts`.	Valeurs possibles : 1 – 180 (min). Valeur par défaut : 5 minutes.
`ProhibitOnScreenKeyboard`	Activation ou désactivation de l'interdiction d'utiliser le clavier virtuel pour l'autorisation de clavier des appareils USB.	`Yes` : l'application interdit l'utilisation du clavier virtuel pour autoriser les appareils USB à partir desquels il est impossible de saisir un code d'autorisation de clavier. `No` (par défaut) : l'application n'interdit pas l'utilisation du clavier virtuel pour autoriser les appareils USB à partir desquels il est impossible de saisir un code d'autorisation de clavier.
`ProhibitBarcodeScanner`	Active ou désactive l'affichage du code d'autorisation sous forme de code-barres pour l'autorisation des appareils USB qui ne permettent pas de saisir un code d'autorisation.	`Yes` (valeur par défaut) interdit l'affichage du code d'autorisation sous forme de code-barres. `No` autorise l'affichage du code d'autorisation sous forme de code-barres.

Protection des connexions réseau et des moyens de communications

Tâche de protection contre les menaces Internet

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces Internet à l'aide de la tâche prédéfinie Protection contre les menaces Internet (`Web_Threat_Protection`).

La tâche s'exécute automatiquement si l'un des navigateurs pris en charge est détecté sur le système et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas défini dans les propriétés de la stratégie). Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la protection contre les menaces Internet en modifiant les paramètres de la tâche prédéfinie Protection contre les menaces Internet.

Paramètres de la tâche de protection contre les menaces Internet

Paramètre	Description	Valeurs
`ActionOnDetect`	Spécifie l'action à effectuer lors de la détection d'un objet infecté dans le trafic Internet.	`Notify` : autorise le téléchargement de l'objet détecté, affiche une notification concernant la tentative d'accès bloqué et crée une entrée de journal avec des informations sur l'objet infecté. `Block` (valeur par défaut) : bloque l'accès à l'objet détecté, affiche une notification concernant la tentative d'accès bloqué et crée une entrée de journal avec des informations sur l'objet infecté.
`CheckMalicious`	Vérification des liens par rapport à la base de données d'adresses Internet malveillantes.	`Yes` (valeur par défaut) : vérifie si les liens sont répertoriés dans la base de données des adresses Internet malveillantes. `No` : ne vérifie pas si les liens sont répertoriés dans la base de données des adresses Internet malveillantes.
`CheckPhishing`	Vérification des liens par rapport à la base de données d'adresses Internet de phishing.	`Yes` (valeur par défaut) : vérifie si les liens figurent dans la base de données des adresses Internet de phishing. `No` : ne vérifie pas si les liens figurent dans la base de données des adresses Internet de phishing.
`UseHeuristicForPhishing`	Utilisation de l'analyse heuristique pour vérifier les pages Web à la recherche de liens de phishing. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` (valeur par défaut) : détecte les liens de phishing à l'aide de l'analyse heuristique. Si cette valeur est spécifiée, le niveau de l'analyse heuristique est `Light` (faible) (l'analyse la moins approfondie avec une charge minimale sur le système). Vous ne pouvez pas modifier le niveau de l'analyse heuristique pour la tâche de protection contre les menaces Internet. `No` : ne détecte pas les liens de phishing à l'aide de l'analyse heuristique.
`CheckAdware`	Vérification des liens par rapport à la base de données des adresses Internet publicitaires.	`Yes` : vérifie si les liens sont répertoriés dans la base de données des adresses Internet publicitaires. `No` (valeur par défaut) : ne vérifie pas si les liens sont répertoriés dans la base de données des adresse Internet publicitaires.

Paramètre	Description	Valeurs
`CheckOther`	Vérification des liens par rapport à la base de données d'adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.	`Yes` : vérifie si des liens sont répertoriés dans les bases de données d'adresses Internet contenant des applications légitimes pouvant être utilisées par des criminels pour endommager vos appareils ou vos données. `No` (valeur par défaut) : ne vérifie pas si des liens sont répertoriés dans les bases de données d'adresses Internet contenant des applications légales pouvant être utilisées par des criminels pour endommager vos appareils ou vos données.
`UseTrustedAddresses`	Utilisation de la liste des adresses Internet fiables. L'application ne vérifie pas les adresses Internet de confiance à la recherche de virus et autres objets malveillants. Vous pouvez spécifier des adresses Internet approuvées à l'aide du paramètre `TrustedAddresses.item_#`.	`Yes` (valeur par défaut) : utilise une liste d'adresses Internet de confiance. `No` : n'utilise pas de liste d'adresses Internet de confiance.
`TrustedAddresses.item_#`	Adresses Internet de confiance.	La valeur par défaut n'est pas définie. Vous pouvez utiliser des masques pour spécifier des adresses Internet. L'utilisation de masques dans le but de définir des adresses IP n'est pas prise en charge.

Articles utiles

Comment spécifier des masques

Lors de la création d'un masque d'adresse, vous pouvez saisir l'astérisque (*) comme caractère générique pour un ou plusieurs caractères. Si vous saisissez ainsi le masque d'adresse *abc*, il sera appliqué à toutes les ressources Internet contenant la séquence abc (par exemple, www.virus.com/download_virus/page_0-9abcdef.html). Pour inclure l'astérisque dans le masque d'adresse en tant que caractère et non en tant que masque, saisissez deux fois le caractère * (par exemple, www.virus.com/**/page_0-9abcdef.html signifie www.virus.com/*/page_0-9abcdef.html).

Analyse du trafic réseau

La ligne de commande fournit des commandes de gestion spéciales pour gérer les paramètres d'analyse du trafic réseau. À l'aide des commandes de gestion des paramètres d'analyse du trafic réseau, vous pouvez :

- Configurer les paramètres d'analyse du trafic réseau.
- Afficher les exclusions depuis l'analyse des connexions chiffrées.
- Effacer la liste des domaines que l'application a automatiquement exclus de l'analyse.
- Configurer la liste des certificats racines de confiance que l'application utilise lors de la vérification des connexions chiffrées.
- Configurer et consulter les exclusions de l'interception du trafic.

Affichage et modification des paramètres de vérification du trafic réseau

À l'aide des commandes spéciales de gestion des paramètres d'analyse du trafic réseau, vous pouvez :

- Afficher les valeurs actuelles des paramètres d'analyse du trafic réseau vers la console ou vers un fichier de configuration. Vous pouvez utiliser ce fichier pour modifier les paramètres.
- Modifier tous les paramètres d'analyse du trafic réseau à l'aide du fichier de configuration. Vous pouvez obtenir le fichier de configuration à l'aide de la commande d'affichage des paramètres d'analyse du trafic réseau.
- Modifiez les paramètres individuels à l'aide d'options de ligne de commande au format `< nom du paramètre >= < valeur du paramètre >`. Vous pouvez obtenir les valeurs actuelles des paramètres à l'aide de la commande pour afficher les paramètres d'analyse du trafic réseau.

Pour afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à la console, exécutez la commande suivante :

```
kesl-control --get-net-settings [--json]
```

Où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à un fichier, exécutez la commande suivante :

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

où :

- `--file <path to the configuration file>` est le chemin d'accès au fichier dans lequel les paramètres d'analyse du trafic réseau seront enregistrés. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour modifier les valeurs des paramètres d'analyse du trafic réseau à l'aide d'un fichier de configuration :

1. Générez les paramètres de l'analyse du trafic réseau dans le fichier de configuration comme décrit ci-dessus.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande:

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

où :

- `--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration contenant les paramètres d'analyse du trafic réseau.
- `--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres d'analyse du trafic réseau spécifiées dans le fichier seront importées dans l'application.

Pour modifier les paramètres d'analyse du trafic réseau à l'aide de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

où `<parameter name>=<parameter value>` correspond au nom et à la valeur d'un paramètre d'analyse du trafic réseau.

Les valeurs des paramètres spécifiés seront modifiées.

Affichage des exclusions liées à l'analyse des connexions chiffrées

Vous pouvez afficher les listes suivantes d'exclusions à l'analyse des connexions chiffrées :

- liste des exclusions ajoutées par l'utilisateur ;
- liste des exclusions ajoutées par l'application ;
- une liste des exclusions reçues des bases de données de l'application.

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées qui ont été ajoutées par une application, exécutez la commande suivante :

```
kesl-control -N --query user
```

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées qui ont été ajoutées par une application, exécutez la commande suivante :

```
kesl-control -N --query auto
```

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées reçues des bases de données de l'application, exécutez la commande suivante :

```
kesl-control -N --query kl
```

Pour effacer une liste de domaines que l'application a automatiquement exclus d'une analyse, exécutez la commande suivante :

```
kesl-control [-N] --clear-web-auto-excluded
```

Gestion de la liste des certificats racines de confiance

Pour ajouter un certificat à la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --add-certificate <path to the certificate>
```

où :

`<path to the certificate>` est le chemin d'accès au fichier de certificat que vous voulez ajouter (au format PEM ou DER).

Pour supprimer un certificat de la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --remove-certificate <subject of the certificate>
```

Pour consulter la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --list-certificates
```

Les informations suivantes sont affichées pour chaque certificat :

- Objet du certificat
- numéro de série du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- empreinte digitale du certificat SHA256.

Configuration et affichage des exclusions à l'interception du trafic

Pour ajouter une exclusion à l'interception du trafic, exécutez la commande :

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination
port>
```

où :

- `<in|out>` correspond au sens du trafic dans la connexion exclue. Vous pouvez configurer une exclusion pour le trafic entrant ou pour le trafic sortant.
- `<remote IP address>` est l'adresse IPv4 ou IPv6 de l'appareil distant. Selon le sens du trafic, le trafic provenant de l'adresse IP spécifiée (exclusion du trafic entrant) ou le trafic vers l'adresse IP spécifiée (exclusion de trafic sortant) sera exclu.
- `<destination port>` correspond, selon le sens du trafic, à ce qui suit :
  - Port sur l'appareil protégé (sauf pour le trafic entrant). Le trafic vers ce port provenant des appareils à distance sera exclu de l'interception.
  - Port sur l'appareil à distance (sauf pour le trafic sortant). Le trafic vers ce port provenant de l'appareil protégé sera exclu de l'interception.

Vous pouvez spécifier uniquement l'adresse IP de l'appareil à distance ou uniquement le port de destination dans l'exclusion.

Si vous spécifiez uniquement l'adresse IP de l'appareil à distance (sans spécifier le port sur l'appareil protégé) dans l'exclusion pour le trafic entrant, tout le trafic provenant de l'appareil à distance est exclu de l'interception. Il est recommandé de configurer une telle exclusion uniquement pour le trafic provenant d'appareils auxquels vous faites confiance.

Pour afficher la liste des exclusions configurées à partir de l'interception du trafic, exécutez la commande :

```
kesl-control --list-bypass-endpoints
```

Les informations suivantes sont affichées pour chaque exclusion :

- numéro de série de l'exclusion ;
- direction de circulation dans la connexion ;
- Adresse IP de l'appareil à distance ;
- numéro de port.

Pour supprimer l'exclusion à l'interception du trafic, exécutez la commande :

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

où :

- `<in|out>` correspond au sens du trafic dans la connexion exclue.
- `<remote IP address` est l'adresse IPv4 ou IPv6 de l'appareil distant dont le trafic est exclu de l'interception (selon la direction du trafic).
- `<destination port>` est un port sur l'appareil protégé (exclusion pour le trafic entrant) ou un port sur l'appareil distant (exclusion pour le trafic sortant).

Tâche de protection contre les menaces réseau

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces réseau à l'aide de la tâche prédéfinie Protection contre les menaces réseau (`Network_Threat_Protection`).

Par défaut, la tâche de protection contre les menaces réseau n'est pas lancée. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la protection contre les menaces réseau en modifiant les paramètres de la tâche prédéfinie Protection contre les menaces réseau.

Paramètres de la tâche de protection contre les menaces réseau

Paramètre	Description	Valeurs
`ActionOnDetect`	Action exécutée en cas de détection d'une activité réseau caractéristique des attaques réseau. La modification de ce paramètre de `Block` à `Notify` efface la liste des appareils bloqués.	`Notify` : autorise l'activité réseau, consigne dans le journal les informations sur l'activité réseau détectée. Si cette valeur est spécifiée, la valeur du paramètre `BlockAttackingHosts` est ignorée. `Block` (valeur par défaut) : bloquer l'activité réseau et consigne dans le journal les informations la concernant.
`BlockAttackingHosts`	Blocage de l'activité réseau à partir des appareils attaquants.	`Yes` (valeur par défaut) : bloquer l'activité réseau de l'appareil attaquant. `No` – ne pas bloquer l'activité réseau de l'appareil attaquant. Si cette valeur est spécifiée et que le paramètre `ActionOnDetect` est défini sur `Block`, l'application bloque l'activité réseau de l'appareil attaquant, mais n'ajoute pas l'appareil à la liste des appareils bloqués.
`BlockDurationMinutes`	Spécifie la durée de blocage des attaques contre les appareils (en minutes).	1 – 32768 Valeur par défaut : 60.
`UseExcludeIPs`	Utilisation d'une liste d'adresses IP dont l'activité réseau ne sera pas bloquée en cas de détection d'une attaque réseau. L'application enregistrera dans le journal uniquement les informations sur les activités malveillante de ces applications. Vous pouvez ajouter des adresses IP à la liste d'exclusion à l'aide du paramètre `ExcludeIPs.item_#`.	`Yes` : utilise une liste d'exclusion d'adresses IP. `No` : (valeur par défaut) : n'utilise pas de liste d'exclusion d'adresses IP.
`ExcludeIPs.item_#`	Spécifie une adresse IP dont l'activité réseau ne sera pas bloquée par l'application. Par défaut, la liste est vide.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. La valeur par défaut n'est pas définie.

Gestion du pare-feu

Sur la ligne de commande, vous pouvez configurer la gestion du pare-feu à l'aide de la tâche prédéfinie de gestion du pare-feu (`Firewall_Management`).

Par défaut, la tâche Gestion du pare-feu n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres de gestion du pare-feu en modifiant les paramètres de la tâche prédéfinie Gestion du pare-feu.

Vous pouvez également configurer les paramètres de gestion du pare-feu à l'aide des commandes de gestion du pare-feu :

- Créer et supprimer des règles de paquets réseau et modifier leur priorité d'exécution.
- Générer une liste des adresses IP ou des sous-réseaux dans les zones réseau.
- Affichez les règles du Firewall créées dans l'application à l'aide de la commande suivante :

```
kesl-control -F --query
```

Paramètres de Gestion du pare-feu

Paramètre	Description	Valeurs
`DefaultIncomingAction`	L'action par défaut à exécuter sur une connexion entrante, si aucune règle réseau ne peut être appliquée à ce type de connexion.	`Allow` (valeur par défaut) : autorise les connexions entrantes. `Block` : bloquer la connexion entrante.
`DefaultIncomingPacketAction`	L'action par défaut à exécuter sur un paquet entrant, si aucune règle de paquet réseau ne peut être appliquée à ce type de connexion.	`Allow` (valeur par défaut) : autorise les paquets entrants. `Block` : bloquer le paquet entrant.
`OpenNagentPorts`	Ajout de règles dynamiques pour l'Agent d'administration aux règles de paquets.	`Yes` (valeur par défaut) : ajoute des règles dynamiques pour l'Agent d'administration aux règles de paquets. `No` : n'ajoute des règles dynamiques pour l'Agent d'administration aux règles de paquets.
La section **[PacketRules.item_#]** définit les règles de paquet réseau de la tâche Gestion du pare-feu. Vous pouvez définir plusieurs sections `[PacketRules.item_#]` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Chaque section `[PacketRules.item_#]` contient les paramètres suivants :		
`Name`	Le nom de la règle de paquet réseau.	Valeur par défaut : `Packet rule #<n>`, où n est un index.
`FirewallAction`	Action à réaliser sur les connexions définies dans cette règle de paquet réseau.	`Allow` (valeur par défaut) : autorise les connexions réseau. `Block` : bloquer la connexion réseau.

`Protocol`	Type de protocole pour lequel l'activité réseau doit être contrôlée.	`Any` (valeur par défaut) : la tâche de gestion du pare-feu contrôle toute l'activité réseau.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

Paramètre	Description	Valeurs
`RemotePorts`	Numéros de port des appareils à distance entre lesquels la connexion doit être contrôlée. Vous pouvez spécifier la valeur sous forme d'entier ou d'intervalle. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `TCP` ou `UDP`.	`Any` (valeur par défaut) : contrôle tous les ports distants. `0` : `65535`.
`LocalPorts`	Numéros de port des appareils locaux entre lesquels la connexion doit être contrôlée. Vous pouvez spécifier la valeur sous forme d'entier ou d'intervalle. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `TCP` ou `UDP`.	`Any` (valeur par défaut) : contrôle tous les ports locaux. `0` : `65535`.
`ICMPType`	Type de paquet ICMP. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `ICMP` ou `ICMPv6`.	`Any` (valeur par défaut) : contrôle tous les types de paquet ICMP. Entier nombre en fonction d'une spécification du protocole de transfert de données.
`ICMPCode`	Code du paquet ICMP. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `ICMP` ou `ICMPv6`.	`Any` (valeur par défaut) : contrôle tous les codes des paquets ICMP. Entier nombre en fonction d'une spécification du protocole de transfert de données.
`Direction`	Direction de l'activité réseau contrôlée.	`IncomingOutgoing` ou `InOut` (valeur par défaut) : contrôle les connexions entrantes et sortantes. `Incoming` ou `In` : contrôler uniquement les connexions entrantes. `Outgoing` ou `Out` : contrôler uniquement les connexions sortantes. `IncomingPacket` ou `InPacket` : contrôler uniquement les paquets entrants. `OutgoingPacket` ou `OutPacket` : contrôler uniquement les paquets sortants. `IncomingOutgoingPacket` ou `InOutPacket` : contrôle les paquets entrants et sortants.
`RemoteAddress`	Adresses réseau des appareils distants qui peuvent envoyer et recevoir des paquets réseau.	`Any` (valeur par défaut) : contrôle les paquets réseau envoyés et/ou reçus par des appareils distants possédant n'importe quelle adresse IP. `Trusted` : zone réseau prédéfinie pour les réseaux de confiance. `Local` : zone réseau prédéfinie pour les réseaux locaux. `Public` : zone réseau prédéfinie pour les réseaux publics. `d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d – d.d.d.d` : plage d'adresses de la version IPv4. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` : plage d'adresses de la version IPv6. x:x:x:x:x:x:x:x/p : sous-réseau d'adresse de la version IPv6, où p est un nombre compris entre 0 et 128, vous pouvez utiliser **::** pour l'abréviation.

Paramètre	Description	Valeurs
`LocalAddress`	Adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.	`Any` (valeur par défaut) : contrôle les paquets réseau envoyés et/ou reçus par des appareils locaux possédant n'importe quelle adresse IP. `d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d – d.d.d.d` : plage d'adresses de la version IPv4. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` : plage d'adresses de la version IPv6. x:x:x:x:x:x:x:x/p : sous-réseau d'adresse de la version IPv6, où p est un nombre compris entre 0 et 128, vous pouvez utiliser **::** pour l'abréviation.
`LogAttempts`	Incluez un enregistrement dans le rapport d'action des règles de réseau.	`Yes` : enregistrer les actions dans un rapport. `No` (valeur par défaut) : ne pas enregistrer les actions dans un rapport.
La section **[NetworkZonesPublic]** contient les adresses réseau associées aux réseaux publics. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : "" (pas d'adresses réseau dans cette zone).
La section **[NetworkZonesLocal]** contient les adresses réseau associées aux réseaux locaux. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : `""` (pas d'adresses réseau dans cette zone).
La section **[NetworkZonesTrusted]** contient les adresses réseau associées aux réseaux de confiance. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : `""` (pas d'adresses réseau dans cette zone).

Configuration de la liste des règles pour les paquets réseau

Pour ajouter une règle de paquet réseau, exécutez la commande suivante :

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

où :

- `--name <rule name>` est le nom de la règle de paquet réseau.
- `--action <Allow|Block>` est l'action à réaliser sur les connexions définies dans cette règle de paquet réseau.
- `--protocol <protocol>` est le protocole pour lequel vous souhaitez surveiller l'activité réseau.
- `--direction <direction>` est la direction de l'activité réseau surveillée.
- `--remote <remote address>:<port>` est l'adresse réseau de l'appareil distant. Vous pouvez spécifier le nom d'une zone réseau prédéfinie comme adresse distante.
- `--local <local address>:<port>` est l'adresse réseau de l'appareil sur lequel Kaspersky Endpoint Security est installé.
- `--at <index>` est l'index de la règle dans la liste des règles de paquets réseau. Si le commutateur `--at` n'est pas spécifié ou si sa valeur est supérieure au nombre de règles dans la liste, la nouvelle règle est ajoutée à la fin de la liste.

Les paramètres pour lesquels vous ne spécifiez pas de valeurs dans la commande sont définis sur les valeurs par défaut.

Exemple de création d'une règle qui bloque toutes les connexions entrantes et établies au port TCP 23

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Exemple de création d'une règle qui bloque les connexions entrantes et établies via le port TCP 23 pour la zone réseau Public

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

Pour supprimer une règle de paquet réseau, exécutez une des commandes suivantes :

```
kesl-control --del-rule --name <rule name>
```

ou

```
kesl-control --del-rule --index <current index>
```

où :

- `--name <rule name>` est le nom de la règle de paquet réseau.
- `--index <current index>` est l'index actuel de la règle dans la liste des règles de paquets réseau.

Si la liste des règles de paquets réseau contient plusieurs règles portant le même nom ou ne contient pas de règle portant le nom ou l'index spécifié, une erreur se produit.

Pour modifier la priorité d'exécution d'une règle pour le paquet réseau, exécutez l'une des commandes suivantes :

```
kesl-control --move-rule --name <rule name> --at < new index>
```

ou

```
kesl-control --move-rule --index <current index> --at <new index>
```

où :

- `--name <rule name>` est le nom de la règle de paquet réseau.
- `--index <current index>` est l'index actuel de la règle dans la liste des règles de paquets réseau.
- `--at <new index>` est le nouvel index de la règle dans la liste des règles de paquets réseau.

Configuration des zones réseau

Pour ajouter une adresse réseau à la zone, exécutez la commande suivante :

```
kesl-control --add-zone <zone> --address <address>
```

où :

- `<zone>` est le nom prédéfini de la zone réseau. Valeurs possibles : `Public`, `Local`, `Trusted`.
- `<address>` est l'adresse réseau ou le sous-réseau.

Pour supprimer une adresse réseau d'une zone, exécutez l'une des commandes suivantes :

```
kesl-control --del-zone <zone> --address <address>
```

ou

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

Si une zone contient plusieurs éléments porteur de la même adresse réseau, la commande `--del-zone` n'est pas exécutée.

Si l'adresse réseau ou l'index indiqués n'existent pas, un message d'erreur s'affiche.

Contrôles de sécurité

Tâche Contrôle des appareils

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Contrôle des appareils (`Device_Control`).

Paramètres du Contrôle des appareils

Paramètre	Description	Valeurs
`OperationMode`	Mode de fonctionnement de l'application lors de la tentative d'accès à un appareil dont l'accès est interdit conformément aux paramètres du Contrôle des appareils.	`Block` (valeur par défaut) : l'application applique le mode d'accès spécifié pour l'appareil ou le bus. `Notify` : l'application teste le mode d'accès sélectionné et génère un événement sur la détection d'une tentative d'accès à l'appareil.
`AllowToRequestTemporaryAccess`	Autorisation de demander un accès temporaire à un appareil verrouillé. L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.1 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.	`Yes` – autoriser l'utilisateur à demander un accès temporaire à l'appareil bloqué dans l'interface graphique de l'application ou sur la ligne de commande. `No` (valeur par défaut) : interdire l'utilisateur à demander un accès temporaire à un appareil verrouillé.
La section **[DeviceClass]** contient les modes d'accès aux appareils en fonction de leur type.		
`HardDrive`	Spécifie le mode d'accès pour les disques durs connectés à l'appareil client.	`Allow` : l'accès à tous les disques durs est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au disque dur dépend du mode d'accès du bus de connexion sur lequel le disque est connecté. `Block` : l'accès à tous les disques durs (à l'exclusion des disques durs système, qui ne sont jamais bloqués par le Contrôle des applications) est bloqué pour les utilisateurs. `ByRule` : l'accès aux disques durs dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux disques durs, l'écriture est interdite.
`RemovableDrive`	Spécifie le mode d'accès aux disques amovibles connectés à l'appareil client.	`Allow` : l'accès à tous les disque amovibles est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à un disque amovible dépend du mode d'accès du bus de connexion sur lequel le disque est connecté. `Block` : l'accès à tous les disques amovibles est bloqué pour les utilisateurs. `ByRule` : l'accès aux disques amovibles dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux disques amovibles, l'écriture est interdite.

Paramètre	Description	Valeurs
`FloppyDrive`	Spécifie le mode d'accès aux lecteurs de disquettes connectés à l'appareil client. L'application ne bloque pas les lecteurs de disquette connectés à un appareil client via le bus ISA.	`Allow` : l'accès à tous les lecteurs de disquette est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de disquette dépend du mode d'accès du bus de connexion sur lequel la disquette est connectée. `Block` : l'accès à tous les lecteurs de disquette est bloqué pour les utilisateurs. `ByRule` : l'accès aux lecteurs de disquette dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux lecteurs de disquettes uniquement, l'écriture est interdite.
`OpticalDrive`	Spécifie le mode d'accès pour les lecteurs CD/DVD connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs CD/DVD est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de CD/DVD dépend du mode d'accès du bus de connexion via lequel le lecteur de CD/DVD est connecté. `Block` : l'accès à tous les lecteurs de CD / DVD est bloqué pour les utilisateurs. `ByRule` : l'accès aux lecteurs CD/DVD dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux lecteurs de CD/DVD, l'écriture est interdite.
`SerialPortDevice`	Spécifie le mode d'accès aux appareils connectés à l'appareil client via un port série. L'application ne bloque pas les appareils connectés à l'appareil client via un port série via le bus ISA.	`Allow` : l'accès aux appareils connectés via un port série est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil connecté via un port série dépend du mode d'accès pour le bus de connexion. `Block` : l'accès aux appareils connectés via un port série est bloqué pour les utilisateurs.
`ParallelPortDevice`	Spécifie le mode d'accès aux appareils connectés à l'appareil client via un port parallèle.	`Allow` : l'accès aux appareils connectés via un port parallèle est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil connecté via un port parallèle dépend du mode d'accès pour le bus de connexion. `Block` : l'accès aux appareils connectés via un port parallèle est bloqué pour les utilisateurs.
`Printer`	Spécifie le mode d'accès aux imprimantes connectées à l'appareil client.	`Allow` : l'accès à toutes les imprimantes est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'imprimante dépend du mode d'accès du bus de connexion via lequel l'imprimante est connectée. `Block` : l'accès à toutes les imprimantes est bloqué pour les utilisateurs.
`Modem`	Spécifie le mode d'accès aux modems connectés à l'appareil client.	`Allow` : l'accès à tous les modems est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au modem dépend du mode d'accès du bus de connexion via lequel le modem est connecté. `Block` : l'accès à tous les modems est bloqué pour les utilisateurs.
`TapeDrive`	Spécifie le mode d'accès aux lecteurs de bande connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs de bande est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au streamer dépend du mode d'accès du bus de connexion via lequel le streamer est connecté. `Block` : l'accès à tous les lecteurs de bande est bloqué pour les utilisateurs.

Paramètre	Description	Valeurs
`MultifuncDevice`	Spécifie le mode d'accès aux dispositifs multifonctions connectés à l'appareil client.	`Allow` : l'accès à tous les appareils multifonctions est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil multifonction dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils multifonctions est bloqué pour les utilisateurs.
`SmartCardReader`	Spécifie le mode d'accès aux lecteurs de cartes à puce connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs de cartes à puce est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de carte à puce dépend du mode d'accès au bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les lecteurs de cartes à puce est bloqué pour les utilisateurs.
`WiFiAdapter`	Spécifie le mode d'accès aux adaptateurs Wi-Fi connectés à l'appareil client.	`Allow` : l'accès à tous les adaptateurs Wi-Fi est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur Wi-Fi dépend du mode d'accès pour le bus de connexion. `Block` : l'accès à tous les adaptateurs Wi-Fi est bloqué pour les utilisateurs.
`NetworkAdapter`	Spécifie le mode d'accès aux adaptateurs réseau connectés à l'appareil client.	`Allow` : l'accès à toutes les cartes réseau est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur réseau externe dépend du mode d'accès au bus de connexion sur lequel l'adaptateur est connecté. Le Contrôle des appareils ne vous permet pas de refuser l'accès aux adaptateurs réseau externes pour éviter de déconnecter votre appareil client du réseau.
`PortableDevice`	Spécifie le mode d'accès aux appareils mobiles connectés à l'appareil client.	`Allow` : l'accès à tous les appareils portables est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil portable dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils portables est bloqué pour les utilisateurs.
`BluetoothDevice`	Spécifie le mode d'accès aux dispositifs Bluetooth connectés à l'appareil client.	`Allow` : l'accès à tous les appareils Bluetooth est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil Bluetooth dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils Bluetooth est bloqué pour les utilisateurs.
`ImagingDevice`	Spécifie le mode d'accès aux appareils d'imagerie connectés à l'appareil client.	`Allow` : l'accès à tous les appareils de traitement d'images est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil d'imagerie dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils de traitement d'images est bloqué pour les utilisateurs.
`SoundAdapter`	Spécifie le mode d'accès aux cartes sons connectées à l'appareil client.	`Allow` : l'accès à toutes les cartes audio est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur audio dépend du mode d'accès au bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à toutes les cartes audio est interdit pour les utilisateurs.

Paramètre	Description	Valeurs
`InputDevice`	Spécifie le mode d'accès aux appareils de saisie (claviers, souris, pavé tactile et autres) connectés à l'appareil client.	`Allow` : l'accès à tous les appareils d'entrée est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil de saisie dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils d'entrée est bloqué pour les utilisateurs.
La section **[DeviceBus]** contient les modes d'accès aux bus de connexion.		
`USB`	Mode d'accès pour les appareils connectés à l'appareil client via l'interface USB.	`Allow` (valeur par défaut) : l'accès à tous les appareils USB est autorisé pour les utilisateurs. `Block` : l'accès à tous les appareils USB est bloqué pour les utilisateurs.
`FireWire`	Mode d'accès pour les appareils connectés à l'appareil client via l'interface FireWire.	`Allow` (valeur par défaut) : l'accès aux appareils connectés via l'interface FireWire est autorisé pour les utilisateurs. `Block` : l'accès aux appareils connectés via l'interface FireWire est bloqué pour les utilisateurs.
La section **[TrustedDevices.item_#]** contient les appareils de confiance.		
`DeviceId`	Spécifie l'ID ou le masque d'ID d'un appareil de confiance.	Vous pouvez utiliser le caractère générique * (n'importe quelle séquence de caractères) ou ? (n'importe quel caractère) pour indiquer l'ID de l'appareil. Exemples : *Pour refuser l'accès à tous les appareils USB à l'exception de celui que vous définissez, indiquez les paramètres suivants :* Dans la section `[DeviceBus]`, le paramètre `USB=Block` Dans la section `[TrustedDevices.item_#]`, le paramètre `DeviceId=<device ID>` *Pour refuser l'accès à tous les appareils USB, mais autoriser l'accès à toutes les clés USB, indiquez les paramètres suivants :* Dans la section `[DeviceBus]`, le paramètre `USB=Block` Dans la section `[TrustedDevices.item_#]`, le paramètre `DeviceId=USBSTOR*`
`Comment`	Commentaire sur l'appareil de confiance spécifié.	—
La section **[TrustedDevices.item_#.Principals.item_#]** contient les règles d'accès à un appareil de confiance.		
`Principal`	L'utilisateur ou le groupe d'utilisateurs pour lesquels l'appareil est approuvé. Si le type d'accès à l'appareil est défini sur lecture seule, lorsque vous attribuez un appareil deconfiance à un utilisateur spécifique, l'utilisateur attribué est ignoré et l'appareil devient accessible en écriture par tous les utilisateurs.	`\Everyone` (valeur par défaut) : l'appareil sera approuvé par tous les utilisateurs. `<user name>` est le nom d'un utilisateur local ou de domaine pour lequel l'appareil est approuvé (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format <nom de domaine>\`<user name>` ou `<user name>` @<nom de domaine>). `@<group name>` est le nom du groupe d'utilisateurs (local ou de domaine) pour lequel l'appareil est approuvé.
La section **[Schedules.item_#]** contient les planifications d'accès pour les appareils. Vous pouvez configurer une programmation uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs CD/DVD.		
`ScheduleName`	Spécifie un nom de planification. Le nom de l'horaire doit être unique.	Valeur par défaut : `Default`. La planification `Default` permet un accès complet aux appareils à tous les utilisateurs à tout moment si l'accès par le bus de connexion est autorisé pour le type d'appareil en question. Vous ne pouvez pas supprimer la planification `Default`.

Paramètre	Description	Valeurs

`DaysHours`	Spécifie des intervalles de temps pour une planification.	`All` (valeur par défaut) : la planification est active 24/7 (aucune limite de temps).
		`<weekday>` : jours de la semaine. Vous pouvez utiliser les noms complets des jours de la semaine ou leurs abréviations (par exemple, pour lundi, vous pouvez spécifier `Mo`, `Mon` ou `Monday`). Pour les jours de la semaine, vous pouvez spécifier des intervalles ou des jours spécifiques. La semaine commence le dimanche.
		`<hour>` – Heures [0:24]. Pour les heures, vous ne pouvez spécifier que des intervalles.
		`Exemple de schedule_1, qui est valide du dimanche au samedi de 0 h à 11 h, de 12 h à 15 h et de 16 h à 24 h.`
		`[Schedules.item_0001]`
		`ScheduleName=schedule_1`
		`DaysHours=Su-Sa:0..11,12..15,16..24`
		`Exemple de schedule_2, qui est valide pour les intervalles suivants : les jeudis de 12 h à 14 h et les vendredis de 2 h à 15 h et de 16 h à 24 h.`
		`[Schedules.item_0002]`
		`ScheduleName=schedule_2`
		`DaysHours=Th:12..14;Fr:2..15,16..24`
		`Exemple de schedule_3, qui est valide 24 heures/24, 7 jours sur 7`
		`[Schedules.item_0003]`
		`ScheduleName=schedule_3`
		`DaysHours=All`

La section **[HardDrivePrincipals.item_ #]** contient les règles d'accès aux disques durs. Pour les disques durs, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un disque dur. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `<user name>` est le nom de l'utilisateur local auquel la règle d'accès s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle d'accès s'applique.
`[HardDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux disques durs est autorisé. `Block` : l'accès aux disques durs est bloqué.
La section **[RemovableDrivePrincipals.item_ #]** contient les règles d'accès aux disques amovibles. Pour les disques amovibles, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un disque amovible. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `<user name>` est le nom de l'utilisateur local auquel la règle d'accès s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle d'accès s'applique.
`[RemovableDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.

Paramètre	Description	Valeurs
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux disques amovibles est autorisé. `Block` : l'accès aux disques amovibles est bloqué.
La section **[FloppyDrivePrincipals.item_ #]** contient les règles d'accès aux disquettes. Pour les lecteurs de disquette, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un lecteur de disquette. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `<user name>` est le nom de l'utilisateur local auquel la règle d'accès s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle d'accès s'applique.
`[FloppyDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (par défaut) : l'accès aux lecteurs de disquette est autorisé. `Block` : l'accès aux lecteurs de disquette est bloqué.
La section **[OpticalDrivePrincipals.item_ #]** contient les règles d'accès aux lecteurs CD/DVD. Pour les lecteurs CD/DVD, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un lecteur CD/DVD. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `<user name>` est le nom de l'utilisateur local auquel la règle d'accès s'applique. `@<group name>` est le nom du groupe d'utilisateurs auquel la règle d'accès s'applique.
`[OpticalDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux lecteurs CD/DVD est autorisé. `Block` : l'accès à tous les lecteurs CD/DVD est bloqué.

Contrôle Internet

Sur la ligne de commande, vous pouvez gérer le Contrôle Internet à l'aide de la tâche prédéfinie Contrôle Internet (`Web_Control`).

La tâche Contrôle Internet est arrêtée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du Contrôle Internet, en modifiant les paramètres de la tâche prédéfinie Contrôle Internet.

Vous pouvez également afficher et configurer les paramètres du Contrôle Internet à l'aide des commandes de gestion du Contrôle Internet.

Tâche Contrôle Internet

Le tableau ci-dessous décrit toutes les valeurs disponibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Contrôle Internet (`Web_Control`).

Paramètres de la tâche Contrôle Internet

Paramètre	Description	Valeurs
`WebControlDefaultAction`	La règle par défaut, c'est-à-dire l'action que Contrôle Internet effectuera lorsqu'il détectera une tentative d'accès à des ressources Web qui ne sont pas couvertes par d'autres règles.	`Allow` (valeur par défaut) : autoriser l'accès aux ressources Web. `Block` : bloque l'accès aux ressources Web.
`ComplaintRecipient`	L'adresse email de l'administrateur pour lui envoyer un message concernant un blocage erroné d'une ressource Web.	
La section **[Rules.item_#]** contient les paramètres suivants :		
`Name`	Le nom de la règle d'accès aux ressources Web. Le nom de la règle doit être unique.	
`WebControlAction`	Action de la règle que le Contrôle Internet exécutera lorsqu'il détectera une tentative d'accès à une ressource Web qui satisfait à la règle.	`Allow` (valeur par défaut) : autoriser l'accès à la ressource Web. `Block` : interdire l'accès à une ressource Web. `Notify` : afficher un avertissement indiquant que la ressource Web n'est pas recommandée à la visite. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.
`Enabled`	État de fonctionnement de la règle d'accès aux ressources Web.	`Yes` : la règle est activée, le Contrôle Internet applique cette règle pendant son fonctionnement. `No` (valeur par défaut) : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle Internet.
`ScheduleId`	Identifiant de calendrier utilisé dans la section `[Schedules.item_#]`.	
`UseUrls`	Utilisation d'un filtre d'adresses de la ressource Web dans une règle.	`Yes` : utiliser un filtre pour les adresses des ressources Web dans une règle. `No` (valeur par défaut) : ne pas utiliser le filtre pour les adresses des ressource Web, appliquer la règle à toutes les adresses des ressources Web.
`Urls.item_#`	L'adresse de la ressource Web, dont l'accès est réglementé par la règle.	Vous pouvez utiliser des masques pour spécifier l'adresse d'une ressource Web.
`UseCategories`	Utilisation de filtres dans une règle par catégories de contenu et par catégories de types de données.	`None` (valeur par défaut) : ne pas utiliser le filtre de contenu des ressources Web. `ContentOnly` : utiliser un filtre par catégories de contenu dans la règle. `FormatOnly` : utiliser un filtre pour les catégories de types de données dans la règle. `ContentAndFormat` : utiliser un filtre dans la règle par catégories de contenu et catégories de types de données.
`[Rules.item_#.ContentCategories.item_#]`	Section pour indiquer la catégorie de contenu.	–

Paramètre	Description	Valeurs
`ContentCategory`	Catégorie de contenu.	`AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, AITools`
`[Rules.item_#.FormatCategories.item_#]`	Section pour spécifier la catégorie de types de données.	–
`FormatCategory`	Catégorie de types de données.	`Video` : vidéo `Audio` : données sonores `OfficeDocument` : fichiers des applications Office `Executable` : fichiers exécutables `Archives` : archives `Images` : fichiers graphiques `Scripts` : scripts
`UsePrincipals`	Utilisation d'un filtre pour les utilisateurs soumis à une règle d'accès aux ressources Web.	`Yes` : utiliser un filtre utilisateur dans la règle. `No` (valeur par défaut) : ne pas utiliser le filtre utilisateur, appliquer la règle à tous les utilisateurs.
`[Rules.item_#.Principals.item_#]`	Section permettant de spécifier les utilisateurs soumis à la règle d'accès aux ressources Web.	
`Name`	Utilisateur ou groupe d'utilisateurs soumis à une règle d'accès aux ressources Web.	`<username>` est le nom de l'utilisateur auquel la règle s'applique. `@<groupname>` est le nom du groupe d'utilisateurs auquel la règle s'applique. Valeur par défaut : la règle d'accès aux ressources Web est appliquée à tous les utilisateurs.
La section **[UrlCategories.item_#]** contient les paramètres suivants :		
`Name`	Nom du groupe d'adresses des ressources Web auquel la règle régule l'accès.	
`Urls.item_#`	L'adresse d'une ressource Web incluse dans le groupe.	Vous pouvez utiliser des masques pour spécifier l'adresse d'une ressource Web.
La section **[Schedules.item_#]** contient le calendrier de fonctionnement d'une règle.		
`Id`	Identifiant de calendrier utilisé dans la section `[Rules.item_#]`.	`1 – 999999` `0` : l'identifiant du calendrier `Default` (par défaut) qui garantit que la règle s'exécute sans restriction de temps, c'est-à-dire à tout moment.

Paramètre	Description	Valeurs
`Name`	Spécifie un nom de planification.	
`DaysHours`	Spécifie des intervalles de temps pour une planification.	`<weekday>` : jours de la semaine. Vous pouvez utiliser les noms complets des jours de la semaine ou leurs abréviations (par exemple, pour lundi, vous pouvez spécifier `Mo`, `Mon` ou `Monday`). Pour les jours de la semaine, vous pouvez spécifier des intervalles ou des jours spécifiques. La semaine commence le dimanche. `<hour>` – Heures [0:24]. Pour les heures, vous ne pouvez spécifier que des intervalles.

Affichage et modification des paramètres de contrôle Internet

Pour afficher les paramètres du Contrôle Internet, exécutez la commande suivante :

```
kesl-control --get-settings 26 [--file <path to the configuration file>] [--json]
```

où :

`--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration vers lequel vous souhaitez exporter les paramètres.

`--json` : afficher les données au format JSON.

Pour modifier les paramètres du Contrôle Internet, exécutez la commande suivante :

```
kesl-control --set-settings 26 [--file <path to the configuration file>] [--json]
```

où :

`--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres.

`--json` : importer les données d'un fichier au format JSON.

Pour supprimer les paramètres configurés et restaurer les paramètres du Contrôle Internet aux valeurs règle par défaut, exécutez la commande suivante :

```
kesl-control --set-settings 26 --set-to-default
```

Contrôle des applications

À partir de la ligne de commande, vous pouvez gérer le contrôle des applications à l'aide de la tâche prédéfinie du contrôle des applications (`Application_Control`).

Par défaut, la tâche Contrôle des applications n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du contrôle des applications sur votre appareil en modifiant les paramètres de la tâche prédéfinie du contrôle des applications.

Si vous modifiez la liste des applications autorisées, ou si vous interdisez le lancement de toutes les applications ou des applications affectant le fonctionnement de Kaspersky Endpoint Security, alors, lors de la modification des paramètres de la tâche à l'aide du fichier de configuration ou des options de ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings --accept
```

Vous pouvez également configurer les paramètres du Contrôle des applications à l'aide des commandes de gestion du Contrôle des applications :

- Créer et modifier les listes des catégories.
- Consulter une liste des catégories créées dans l'application.
- Configurer une liste des règles du Contrôle des applications.

Tâche Contrôle des applications

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Contrôle des applications (`Application_Control`).

Paramètres de la tâche Contrôle des applications

Paramètre	Description	Valeurs
`AppControlMode`	Mode de fonctionnement du module Contrôle des applications.	`AllowList` : Kaspersky Endpoint Security interdit pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. `DenyList` (valeur par défaut) : Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.
`AppControlRulesAction`	Action que l'application Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles configurées :	`ApplyRules` (valeur par défaut) : Kaspersky Endpoint Security applique les règles du contrôle des applications et exécute l'action définie. `TestRules` : Kaspersky Endpoint Security teste les règles et génère un événement concernant la détection d'une application correspondant à la règle.
La section **[Categories.item_#]** contient les paramètres suivants :		
`Name`	Nom de la catégorie d'applications à laquelle la règle va s'appliquer.	
`UseIncludes`	Utilisation de conditions d'inclusion pour le déclenchement de la règle.	`Yes` : appliquer la règle à l'application si celle-ci satisfait à au moins une condition d'inclusion. `No` (valeur par défaut) : ne pas appliquer la règle à l'application, même si celle-ci satisfait à la condition d'inclusion.
`IncludeFileNames.item_#`	Nom du fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des masques pour spécifier le nom du fichier.
`IncludeFolders.item_#`	Nom du répertoire contenant le fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des masques pour spécifier le nom du répertoire.
`IncludeHashes.item_#`	Hachage SHA256 du fichier exécutable pour le déclenchement de la règle.	Seul SHA256 est autorisé.
`UseExcludes`	Utilisation de conditions d'exclusion pour le déclenchement de la règle.	`Yes` : ne pas appliquer la règle à l'application si celle-ci satisfait à au moins une condition d'exclusion ou si elle ne satisfait à aucune règle d'inclusion. `No` (valeur par défaut) : appliquer la règle à l'application, même si celle-ci satisfait à la condition d'exclusion.

Paramètre	Description	Valeurs
`ExcludeFileNames.item_#`	Nom du fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des masques pour spécifier le nom du fichier.
`ExcludeFolders.item_#`	Nom du répertoire contenant le fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des masques pour spécifier le nom du répertoire.
`ExcludeHashes.item_#`	Hachage SHA256 du fichier exécutable pour le déclenchement de la règle.	Seul SHA256 est autorisé.
La section **[AllowListRules.item_#]** contient la liste des règles du Contrôle des applications pour le mode de fonctionnement *Liste d'autorisation* (*AllowList*). Chaque section [AllowListRules.item_#] contient les paramètres suivants :		
`Description`	Description de la règle du Contrôle des applications.	
`AppControlRuleStatus`	État de fonctionnement de la règle du Contrôle des applications.	`On` (valeur par défaut) : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le Contrôle des applications. `Off` : la règle n'est pas utilisée pour contrôler les applications. `Test` : l'application Kaspersky Endpoint Security autorise le lancement des applications soumises à l'action de la règle, mais consigne les informations relatives au lancement de ces applications dans le rapport.
`Category`	Nom de la catégorie des applications à laquelle la règle s'applique. Vous pouvez indiquer en guise de catégorie la catégorie d'applications "Golden Image".	
La section **[AllowListRules.item_#.ACL.item_#]** contient la liste des utilisateurs qui ont le droit ou non de lancer des applications.		
`Access`	Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.	`Allow` (valeur par défaut) : autorise le lancement d'applications. `Block` : interdit le lancement d'applications.
`Principal`	Utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.	`\Everyone` (valeur par défaut) : la règle s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom de l'utilisateur auquel la règle s'applique. `@< nom de groupe >` est le nom du groupe d'utilisateurs auquel la règle s'applique.
La section **[DenyListRules.item_#]** contient la liste des règles du Contrôle des applications pour le mode de fonctionnement *Liste de refus* (*DenyList*). Chaque section [DenyListRules.item_#] contient les paramètres suivants :		
`Description`	Description de la règle du Contrôle des applications.	
`AppControlRuleStatus`	État de fonctionnement de la règle du Contrôle des applications.	`On` (valeur par défaut) : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le Contrôle des applications. `Off` : la règle n'est pas utilisée pour contrôler les applications. `Test` : l'application Kaspersky Endpoint Security autorise le lancement des applications soumises à l'action de la règle, mais consigne les informations relatives au lancement de ces applications dans le rapport.
`Category`	Nom de la catégorie d'applications créée à laquelle la règle s'applique. Vous pouvez indiquer en guise de catégorie la liste d'application "Golden Image".	
La section **[DenyListRules.item_#.ACL.item_#]** contient la liste des utilisateurs qui ont le droit ou non de lancer des applications.		
`Access`	Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.	`Allow` : autoriser le lancement des applications. `Block` (valeur par défaut) : interdit le lancement des applications.

Paramètre	Description	Valeurs
`Principal`	Utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.	`\Everyone` (valeur par défaut) : la règle s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom de l'utilisateur auquel la règle s'applique. `@< nom de groupe >` est le nom du groupe d'utilisateurs auquel la règle s'applique.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Créer et modifier une liste des catégories

Vous pouvez créer une nouvelle catégorie de deux manières :

- en utilisant la commande "kesl --set-settings" et le fichier de configuration des paramètres de la tâche Contrôle des applications (`Application_Control`).
- en utilisant la commande kesl --set-categories et le fichier de configuration des paramètres de la catégorie.

Pour créer des catégories des applications, exécutez la commande suivante :

```
kesl-control --set-categories --file <path to the configuration file>
```

où :

`--file <path to the configuration file>` est le chemin d'accès au fichier de configuration contenant les paramètres des catégories.

Le fichier avec les paramètres de la catégorie doit avoir la structure suivante :

```
[
   {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
```

```
        "Name" : "<category name 2>"
    }
]
```

Pour spécifier le nom du fichier dans les champs `Exclude` et `Include`, vous pouvez utiliser des masques.

Le paramètre `Name` est requis. Si vous ne spécifiez pas le nom de la catégorie, elle ne sera pas créée ou sera supprimée. Le paramètre `GUID` est également requis. Si vous ne le spécifiez pas, un message d'erreur s'affiche et la catégorie n'est pas créée. Le paramètre `GUID` doit être spécifié sans tirets.

Pour modifier la liste des catégories des applications créées, exécutez la commande suivante :

```
kesl-control --set-categories [--names <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

où :

- `<category name 1> <category name 2> ... <category name N>` sont les noms des catégories dont vous souhaitez modifier les informations. Si vous souhaitez modifier les informations sur plusieurs catégories, spécifiez les noms de catégories séparés par un espace. Si vous ne spécifiez pas de nom de catégorie, les catégories existantes seront supprimées et de nouvelles catégories seront créées à partir du fichier spécifié.
- `--file <path to the configuration file>` est le chemin d'accès au fichier de configuration contenant les paramètres des catégories.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Consultation de la liste des catégories

À partir de la ligne de commande, vous pouvez afficher une liste des catégories créées des applications à l'aide de la commande de gestion par le contrôle des applications `kesl-control --get-categories`.

La liste des catégories créées contient les catégories suivantes :

- catégories créées dans Kaspersky Security Center ;
- catégories ajoutées dans les paramètres de la tâche Contrôle des applications via la ligne de commande ;
- catégorie "GoldenImage" créée à l'aide de la tâche Inventaire (dans Kaspersky Security Center ou via la ligne de commande).

Pour afficher la liste de toutes les catégories des applications créées, exécutez la commande suivante :

```
kesl-control --get-categories [--file <path to the configuration file>] [--json]
```

où :

- `--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration vers lequel vous souhaitez exporter les paramètres.
- `--json` : afficher les paramètres au format JSON.

Kaspersky Endpoint Security affiche les informations suivantes sur chaque catégorie des applications :

- identifiant unique (GUID) de la catégorie ;
- nom de la catégorie ;
- une liste des conditions qui incluent les conditions de déclenchement de la règle ;
- Liste des conditions d'exclusion pour le déclenchement de la règle.

Pour afficher la liste des catégories distinctes des applications, exécutez la commande suivante :

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

où :

- `<category name 1> <category name 2> ... <category name N>` sont les noms des catégories pour lesquelles vous souhaitez afficher les informations. Si vous souhaitez consulter des informations sur plusieurs catégories, saisissez les noms des catégories séparés par un espace.
- `--file <path to the configuration file>` – chemin d'accès complet au fichier de configuration au format JSON dans lequel la liste des catégories sera exportée.
- `--json` : afficher les paramètres au format JSON.

Si, dans les paramètres de la tâche Contrôle des applications, dans la section `[Categories.item_#]`, vous avez spécifié des liens symboliques vers le fichier d'application ou vers le répertoire contenant les fichiers exécutables pour les conditions d'inclusion ou d'exclusion du déclencheur de règles, le chemin d'origine auquel le lien symbolique est référencé s'affichera lors de l'affichage de la liste des catégories pour ces conditions.

Configuration de la liste des règles du Contrôle des applications

Pour afficher la liste des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --get-settings 21 [--file <path to the configuration file>] [--json]
```

où :

- `--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration vers lequel vous souhaitez exporter les paramètres.
- `--json` : afficher les données au format JSON.

Kaspersky Endpoint Security affichera les informations suivantes sur les règles du Contrôle des applications :

- Mode de fonctionnement du module Contrôle des applications.
- Action que le Contrôle des applications effectue lors de la détection d'une tentative de lancement d'une application qui correspond à la règle configurée.
- Description de la règle du Contrôle des applications (le cas échéant).
- État de la règle du Contrôle des applications
- Nom de la catégorie d'applications à laquelle la règle s'applique
- Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.
- Utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.

Pour modifier la liste des catégories des applications et des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 [--file <path to the configuration file>] [--json]
```

où :

- `--file <path to the configuration file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres.
- `--json` : importer les données d'un fichier au format JSON.

Pour supprimer la liste des catégories des applications et des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 --set-to-default
```

Configuration de l'inventaire

Depuis la ligne de commande, vous pouvez faire l'inventaire des applications de l'appareil protégé des manières suivantes :

- À l'aide de la tâche prédéfinie Inventaire (`Inventory_Scan`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

- À l'aide des tâches personnalisées d'inventaire (tâches de type `InventoryScan`). Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche.

Vous pouvez afficher la liste des applications découvertes sur un appareil suite à la tâche Inventaire à l'aide des commandes de gestion par le contrôle des applications.

Tâche Inventaire

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche Inventaire (`Inventory_Scan`).

Paramètres de la tâche d'inventaire

Paramètre	Description	Valeurs
`ScanScripts`	Activation de l'analyse des scripts.	`Yes` (valeur par défaut) : analyser les scripts. `No` : ne pas analyser les scripts.
`ScanBinaries`	Activation de l'analyse des fichiers binaires (elf, java, et pyc).	`Yes` (valeur par défaut) : analyser les fichiers binaires. `No` : ne pas analyser les fichiers binaires.
`ScanAllExecutable`	Activation de l'analyse des fichiers avec un bit exécutable.	`Yes` (valeur par défaut) : analyser les fichiers avec un bit exécutable. `No` : ne pas analyser les fichiers avec un bit exécutable.
`GoldenImageAction`	L'action que Kaspersky Endpoint Security doit effectuer sur la catégorie d'applications Golden Image à la fin de la tâche d'inventaire : Vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles de contrôle des applications.	`DoNothing` (valeur par défaut) – ne pas modifier la catégorie d'applications Golden Image une fois l'inventaire effectué. `Create` – ajouter les applications détectées à la catégorie d'applications Golden Image. Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. `Remove` – effacez la catégorie d'applications Golden Image. La catégorie est effacée dès le lancement de la tâche, sans effectuer d'inventaire des fichiers sur l'appareil.
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	Description de la zone d'inventaire. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
`UseScanArea`	Activation de l'analyse de la zone d'inventaire. Pour exécuter la tâche, il faut activer l'analyse d'au moins une zone d'inventaire.	`Yes` (valeur par défaut) : analyser la zone d'inventaire indiquée. `No` : ne pas analyser la zone d'inventaire indiquée.
`AreaMask.item_#`	Restriction de la zone d'inventaire. Dans la zone d'inventaire, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format "shell". Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'inventaire. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. Valeur par défaut : `/usr/bin`
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	Description de la zone d'exclusion de l'inventaire.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone d'inventaire indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion d'inventaire selon des masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'inventaire. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`< chemin d'accès au répertoire local >` exclut les objets du répertoire indiqué de l'analyse. Vous pouvez utiliser des masques pour spécifier le chemin.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Consultation de la liste des applications détectées

Pour consulter la liste des applications détectées sur l'appareil, exécutez la commande suivante :

```
kesl-control --get-app-list [--json]
```

où `--json` : afficher les données au format JSON.

Kaspersky Endpoint Security affiche les informations suivantes sur les applications détectées :

- **Date et heure d'inventaire**. Date et heure d'exécution de la tâche d'inventaire.
- **Nombre d'applications**. Le nombre d'applications trouvées sur l'appareil.

- Liste des applications contenant les informations suivantes :
  - **Chemin d'accès**. Chemin d'accès à l'application.
  - **Hash**. La somme de hash de l'application.
  - **Type**. Type d'application. Par exemple : `Script`, `Executable`.
  - **Catégories**. Les catégories auxquelles l'application appartient (si elles ont été créées auparavant). Vous pouvez afficher la liste des catégories d'applications créées à l'aide de la commande suivante :

    ```
    kesl-control --get-categories
    ```

Lorsqu'une nouvelle catégorie est ajoutée, ses informations dans la liste des applications ne sont pas automatiquement mises à jour. Pour mettre à jour la liste des applications, la tâche Inventaire doit être exécutée à nouveau.

Tâche Contrôle de l'intégrité du système

À partir de la ligne de commande, vous pouvez gérer le contrôle de l'intégrité du système en temps réel à l'aide de la tâche prédéfinie du contrôle de l'intégrité du système (`System_Integrity_Monitoring`). Le type de tâche `OAFIM`.

La tâche Contrôle de l'intégrité du système n'est pas exécutée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du contrôle de l'intégrité du système sur l'appareil en modifiant les paramètres de la tâche prédéfinie Contrôle de l'intégrité du système.

Paramètres de la tâche de contrôle de l'intégrité du système à l'accès

Paramètre	Description	Valeurs
`UseExcludeMasks`	Active l'exclusion de la zone de contrôle des objets définis par le paramètre `ExcludeThreats.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion du contrôle des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez indiquer plusieurs masques. Chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.
La section [ScanScope.item_#] contient les zones de surveillance de la tâche Contrôle de l'intégrité du système. Il faut définir au moins une zone de contrôle pour la tâche. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.	La valeur par défaut n'est pas définie.

Paramètre	Description	Valeurs
`UseScanArea`	Active l'analyse de la zone de contrôle.	`Yes` (valeur par défaut) : surveille la zone indiquée. `No` : ne surveille pas une zone indiquée.
`Path`	Chemin d'accès au répertoire à surveiller.	Vous pouvez utiliser des masques pour spécifier le chemin. Valeur par défaut : /opt/kaspersky/kesl/
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (contrôler tous les objets).
[ExcludedFromScanScope.item_#] contient les objets à exclure de toutes les sections [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone de surveillance indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée de la surveillance. `No` : n'exclut pas la zone indiquée de la surveillance.
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la surveillance.	Vous pouvez utiliser des masques pour spécifier le chemin. La valeur par défaut n'est pas définie.
`AreaMask.item_#`	Restriction de la zone d'exclusion du contrôle. Dans la zone d'exclusion du contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets du contrôle).

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Tâche Vérification de l'intégrité du système

Vous pouvez exécuter une vérification de l'intégrité du système sur un appareil en ligne de commande à l'aide de tâches personnalisées de vérification de l'intégrité du système (`System_Integrity_Monitoring`). Le type de tâche `ODFIM`.

Vous pouvez démarrer, arrêter, suspendre ou reprendre manuellement les tâches définies par l'utilisateur et configurer la planification de la tâche. Vous pouvez configurer les paramètres de vérification de l'intégrité du système en modifiant les paramètres de ces tâches.

Paramètres de la tâche Vérification de l'intégrité du système

Paramètre	Description	Valeurs
`RebuildBaseline`	Activer la mise à jour de l'instantané de l'état du système une fois la tâche *Vérification de l'intégrité du système* terminée.	`Yes` : mettre à jour l'instantané de l'état du système à chaque fois que la tâche *Vérification de l'intégrité du système* est terminée. `No` (par défaut) : ne pas mettre à jour l'instantané de l'état du système à chaque fois que la tâche *Vérification de l'intégrité du système* est terminée.
`CheckFileHash`	Utilisez le hachage du fichier (SHA256) comme critère selon lequel l'état actuel du fichier contrôlé est comparé à l'état d'origine.	`Yes` : vérifier le hachage. `No` (valeur par défaut) : désactive une analyse de hash. Si la vérification est désactivée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique).
`TrackDirectoryChanges`	Active la surveillance des répertoires.	`Yes` : surveiller les répertoires tout en effectuant une vérification de l'intégrité du système. `No` (valeur par défaut) : ne surveille pas les répertoires.
`TrackLastAccessTime`	Active la vérification de l'heure du dernier accès au fichier. Dans les systèmes d'exploitation Linux, c'est le paramètre `noatime`.	`Yes` : vérifie la dernière fois où le fichier a été consulté. `No` (valeur par défaut) : ne vérifie pas la dernière fois où le fichier a été consulté.
`UseExcludeMasks`	Active l'exclusion de la zone de contrôle des objets définis par le paramètre `ExcludeMasks.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion du contrôle des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez indiquer plusieurs masques. Chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.
La section [ScanScope.item_#] contient les zones de surveillance de la *vérification de l'intégrité du système*. Il faut définir au moins une zone de contrôle pour la tâche. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Active l'analyse de la zone de contrôle.	`Yes` (valeur par défaut) : surveille la zone indiquée. `No` : ne surveille pas une zone indiquée.
`Path`	Chemin d'accès au répertoire à surveiller.	Vous pouvez utiliser des masques pour spécifier le chemin. Valeur par défaut : /opt/kaspersky/kesl/

Paramètre	Description	Valeurs
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (contrôler tous les objets).
La section **[ExcludedFromScanScope.item_#]** contient les objets à exclure de toutes les sections [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone de surveillance indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée de la surveillance. `No` : n'exclut pas la zone indiquée de la surveillance.
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la surveillance.	Vous pouvez utiliser des masques pour spécifier le chemin. La valeur par défaut n'est pas définie.
`AreaMask.item_#`	Restriction de la zone d'exclusion du contrôle. Dans la zone d'exclusion du contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets du contrôle).

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Protection contre les menaces avancées et les attaques ciblées

Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

En ligne de commande, vous pouvez gérer l'intégration entre Kaspersky Endpoint Security et la solution Kaspersky Endpoint Detection and Response Expert (on-premises) à l'aide de la tâche prédéfinie *Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)*.

Cette tâche permet également de configurer les paramètres d'intégration avec le module Kaspersky Endpoint Detection and Response (KATA). Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), vous devez sélectionner le mode d'intégration *EDR Expert (on-premises)* et gérer les paramètres d'intégration selon les besoins.

Vous pouvez gérer les paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) en modifiant les paramètres de la tâche prédéfinie.

Par défaut, la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* ne s'exécute pas. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez gérer les certificats utilisés pour la connexion aux serveurs OSMP à l'aide des commandes d'administration du module EDR Expert (on-premises).

Paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Le tableau ci-dessous décrit les paramètres de la tâche prédéfinie Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`), que vous pouvez configurer lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).

Cette tâche permet également de configurer les paramètres d'intégration avec le module Kaspersky Endpoint Detection and Response (KATA). Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), vous devez sélectionner le mode d'intégration *EDR Expert (on-premises)* (`Mode=EDRExpertOnPrem`) dans les paramètres de la tâche.

Paramètres de l'Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security interagit avec des serveurs de la plateforme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` est le mode d'intégration d'EDR Expert (on-premises). Active l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Paramètre	Description	Valeur
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur d'actions de réponse OSMP. Si l'authentification bidirectionnelle est activée sur le serveur de réponse aux menaces OSMP, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur d'actions de réponse aux menaces OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence d'envoi des requêtes de synchronisation au serveur de réponse OSMP (en minutes).	Valeur par défaut : `5`.
`ConnectionTimeout`	Délai d'expiration maximal de la connexion au serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`RequestTimeout`	Délai d'attente maximal d'une réponse du serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`EnableTelemetry`	Envoi des données relatives aux événements sur les appareils (télémétrie) au serveur de collecte de télémétrie OSMP.	`Yes` (valeur par défaut) : envoyer la télémétrie au serveur de collecte de télémétrie OSMP. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur d'actions de réponse OSMP. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur d'actions de réponse OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur d'actions de réponse OSMP.	Valeur par défaut : `443`.
La section **[TelemetrySettings]** contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.		
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur de collecte de télémétrie OSMP. Si l'authentification bidirectionnelle est activée sur le serveur de télémétrie OSMP, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur de télémétrie OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur de collecte de télémétrie OSMP en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente d'une réponse du serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `10`.
`OnlyTaggedEvents`	Envoi de la télémétrie avec IOA uniquement. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements.	`Yes` : envoyer uniquement les données de télémétrie comportant un indicateur d'attaque (Indicator of Attack, IOA). `No` (valeur par défaut) : envoyer toutes la télémétrie.
La section **[TelemetrySettings.Endpoints.item_#]** contient l'adresse et le port du serveur de collecte de télémétrie OSMP. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur de collecte de télémétrie OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.

Paramètre	Description	Valeur
`Port`	Port de connexion au serveur de collecte de télémétrie OSMP.	Valeur par défaut : `443`.
La section **[TelemetrySettings.EventTransferSettings]** contient les paramètres de transfert des données vers le serveur de collecte de télémétrie OSMP.		
`MaximumDataTransferTime`	Délai maximal d'envoi des événements au serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `30`.
`UseRequestCountLimits`	Limitez le nombre de requêtes. Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Gestion des certificats de connexion aux serveurs OSMP EDR Expert (on-premises)

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion aux serveurs OSMP. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer des certificats des serveurs OSMP : serveur d'actions de réponse et serveur de collecte de télémétrie
- afficher des informations sur les certificats de serveurs
- supprimer les certificat des serveurs
- ajouter ou remplacer des certificats client utilisés pour sécuriser les connexions aux serveurs OSMP : serveur de réponse et serveur de collecte de télémétrie
- afficher des informations sur le certificats client
- supprimer les certificats client

Administration des certificats de connexion au serveur d'actions de réponse OSMP

Pour ajouter ou remplacer le certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

où `<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse :

1. Exécutez la commande:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   où `<file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Saisissez le mot de passe du cryptocontainer

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur OSMP si la vérification du certificat client est activée dans les paramètres du serveur OSMP et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)*, le paramètre `UseClientPinnedCertificate` de la section `[KATAEDR]` est défini sur `yes`.

Pour afficher les informations relatives au certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

Pour afficher les informations relatives au certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer le certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

Pour supprimer le certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

Administration des certificats de connexion au serveur de collecte de télémétrie OSMP

Pour ajouter ou modifier un certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

où `<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie :

1. Exécutez la commande:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   où `<file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur OSMP si la vérification du certificat client est activée dans les paramètres du serveur OSMP et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)*, le paramètre `UseClientPinnedCertificate` de la section `[TelemetrySettings]` est défini sur `yes`.

Pour afficher les informations relatives au certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

Pour afficher des informations sur le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

Pour supprimer le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Vous pouvez gérer l'intégration entre Kaspersky Endpoint Security et la solution Kaspersky Endpoint Detection and Response Expert (cloud) à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)* sur la ligne de commande.

Vous pouvez gérer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) en modifiant les paramètres de la tâche prédéfinie.

Par défaut, la tâche *Intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)* n'est pas exécutée. Vous pouvez démarrer et arrêter la tâche manuellement.

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Le tableau suivant décrit les paramètres de la tâche prédéfinie d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) (`EDRExpertCloud`).

Comment obtenir les valeurs actuelles des paramètres de la tâche

```
kesl-control --get-settings 39
```

Comment configurer les paramètres de la tâche

```
kesl-control --set-settings 39 <parameter>=<value>
```

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud)

Paramètre	Description
Paramètres d'intégration du serveur de réponse	
`UseTunnel`	Utilisation d'un tunnel TCP pour la connexion au serveur de réponse. Un tunnel TCP est utilisé pour la connexion au serveur si la stratégie de sécurité de votre infrastructure ne vous permet pas de vous connecter directement aux serveurs. Par défaut, l'utilisation d'un tunnel TCP est désactivée (`No`).
`TunnelAddress`	Adresse du serveur (IPv4 ou IPv6) pour la connexion au tunnel.
`TunnelPort`	Port du serveur pour la connexion au tunnel.
`SynchronizationPeriod`	Fréquence d'envoi des requêtes de synchronisation au serveur de réponse OSMP (en minutes). Valeur par défaut : `5`.
Paramètres d'intégration du serveur de collecte des données de télémétrie La section `[TelemetrySettings]` contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.	

Paramètre	Description
`EnableTelemetry`	Envoi des données relatives aux événements sur les appareils (télémétrie) au serveur de collecte de télémétrie OSMP. L'envoi de la télémétrie est activé par défaut (`Yes`).
`OnlyTaggedEvents`	Envoi de la télémétrie avec IOA uniquement. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements. Par défaut, l'envoi de la télémétrie avec IOA uniquement est désactivé (`No`).
`UseTunnel`	Utilisation d'un tunnel TCP pour la connexion au serveur de collecte de télémétrie. Un tunnel TCP est utilisé pour la connexion au serveur si la stratégie de sécurité de votre infrastructure ne vous permet pas de vous connecter directement aux serveurs. Par défaut, l'utilisation d'un tunnel TCP est désactivée (`No`).
`TunnelAddress`	Adresse du serveur (IPv4 ou IPv6) pour la connexion au tunnel.
`TunnelPort`	Port du serveur pour la connexion au tunnel.
La section `[TelemetrySettings.EventTransferSettings]` contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.	
`UseRequestCountLimits`	Limitez le nombre de requêtes. Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Cette option est désactivée par défaut.
`MaximumDataTransferTime`	Délai maximum lors de l'envoi des événements. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.
`EventLimitExceededPercentage`	Pourcentage de dépassement de la limite d'événements. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

Gestion des certificats de connexion aux serveurs OSMP EDR Expert (cloud)

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

L'application reçoit automatiquement les adresses des serveurs et les certificats permettant d'établir une connexion de confiance une fois que vous avez accepté les conditions du contrat de Kaspersky Endpoint Detection and Response Expert (cloud) relatif au traitement des données. Par conséquent, vous ne pouvez pas ajouter ou supprimer de certificats à l'aide de commandes. Vous pouvez uniquement afficher les informations sur les certificats sur la ligne de commande.

Administration des certificats de connexion au serveur d'actions de réponse OSMP

```
Pour afficher les informations sur le certificat du serveur d'actions de réponse
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

```
Pour afficher les informations sur le certificat client utilisé pour la connexion au serveur d'actions de réponse
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Administration des certificats de connexion au serveur de collecte de télémétrie OSMP

```
Affichage des informations sur le certificat du serveur de collecte de télémétrie
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

```
Pour afficher les informations sur le certificat client utilisé pour la connexion au serveur de collecte de télémétrie
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Intégration à Kaspersky Endpoint Detection and Response (KATA)

En ligne de commande, vous pouvez gérer l'intégration entre Kaspersky Endpoint Security et le module Kaspersky Endpoint Detection and Response (KATA) à l'aide de la tâche prédéfinie *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)*.

Cette tâche vous permet également de gérer les paramètres d'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises). Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration EDR (KATA) dans les paramètres de la tâche et gérer les paramètres d'intégration si nécessaire.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) en modifiant les paramètres d'une tâche prédéfinie.

Par défaut, la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* ne s'exécute pas. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez gérer les certificats utilisés pour la connexion aux serveurs KATA à l'aide des commandes d'administration du module EDR Expert (on-premises).

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Le tableau ci-dessous décrit les paramètres de la tâche prédéfinie Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`), que vous pouvez gérer lors de l'intégration avec Kaspersky Endpoint Detection and Response (KATA).

Cette tâche vous permet également de gérer les paramètres d'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises). Pour intégrer le module Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration *EDR (KATA)* (paramètre `Mode=EDRKATA`) dans les paramètres de la tâche.

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security interagit avec des serveurs de la plateforme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` est le mode d'intégration d'EDR Expert (on-premises). Active l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. Si l'authentification bidirectionnelle est activée côté serveur KATA, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter le certificat client avant de démarrer la tâche.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.

Paramètre	Description	Valeur
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur KATA, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KATA en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur KATA en secondes.	Valeur par défaut : `10`.
`EnableTelemetry`	Envoi des données d'événement (télémétrie) à KATA.	`Yes` (valeur par défaut) : envoie la télémétrie au serveur KATA. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur KATA. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur KATA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur KATA.	Valeur par défaut : `443`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des données vers le serveur KATA.		
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur KATA.	Valeur par défaut : `30`.
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur KATA.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Gestion des certificats pour la connexion au serveur KATA

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur KATA. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur KATA ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur KATA ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

où `<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   où `<file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Saisissez le mot de passe du cryptocontainer

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur KATA si la vérification du certificat client est activée dans les paramètres du serveur KATA et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)*, le paramètre `UseClientPinnedCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat de serveur, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate
```

Pour afficher les informations relatives au certificat client, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Intégration avec Kaspersky Network Detection and Response (KATA)

Vous pouvez gérer, depuis la ligne de commande, l'intégration entre Kaspersky Network Security et Kaspersky Endpoint Detection and Response (KATA) à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Network Detection and Response (KATA) (KATANDR)* :

Par défaut, la tâche I*ntégration avec Kaspersky Network Detection and Response (KATA)* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Network Detection and Response (KATA) en modifiant les paramètres d'une tâche prédéfinie.

Vous pouvez gérer les certificats utilisés pour se connecter aux serveurs NDR à l'aide des commandes d'administration des modules NDR (KATA).

Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)

Le tableau décrit tous les paramètres disponibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Intégration avec Kaspersky Network Detection and Response (KATA) (`KATANDR`).

Paramètres de la tâche Intégration à Kaspersky Network Detection and Response (KATA)

Paramètre	Description	Valeur
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. Si l'analyse du certificat client est activée du côté serveur NDR, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Kaspersky Network Detection and Response (KATA).*	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur NDR en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur NDR en secondes.	Valeur par défaut : `10`.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur NDR.		
`Address`	Adresse du serveur NDR. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur NDR.	Valeur par défaut : `8081`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur NDR.		
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur NDR.	Valeur par défaut : `30`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.

Paramètre	Description	Valeur
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur NDR.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`EventLimitExceededPercentage`	Pourcentage de dépassement de la limite d'événements. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.
`PingPeriod`	Fréquence d'interrogation des serveurs NDR en secondes.	Valeur par défaut : `450`.

Gestion des certificats pour la connexion au serveur NDR

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur NDR. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur NDR ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur NDR ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

où `<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande:

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   où `<file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Saisissez le mot de passe du cryptocontainer

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur NDR si la vérification du certificat client est activée dans les paramètres du serveur NDR et que, dans les paramètres de la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)*, le paramètre `UseClientPinnedCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat de serveur, exécutez la commande suivante :

```
kesl-control [-R] --query-katandr-server-certificate
```

Pour afficher les informations relatives au certificat client, exécutez la commande suivante :

```
kesl-control [-R] --query-katandr-client-certificate
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-R] --remove-katandr-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --remove-katandr-client-certificate
```

Intégration avec Sandbox

Depuis la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec Sandbox à l'aide de la tâche prédéfinie *Intégration avec KATA*.

Par défaut, la tâche *Intégration avec Sandbox* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Pour lancer la tâche Intégration avec Sandbox, exécutez la commande suivante :

```
kesl-control --start-task 29
```

L'exécution de la tâche *Intégration avec Sandbox* est impossible si le certificat du serveur n'est pas ajouté.

Si la tâche *Intégration avec Sandbox* a démarré et si son mode sélectionné permet d'envoyer manuellement des fichiers pour analyse (`Manual` ou `AutoAndManual`), vous pouvez envoyer des fichiers à analyser dans Sandbox depuis la ligne de commande.

Comment envoyer des fichiers à Sandbox pour analyse

```
kesl-control [-X] --sandbox <path>
```

où `<path>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

Vous pouvez configurer les paramètres d'intégration avec Sandbox en modifiant les paramètres d'une tâche prédéfinie.

À l'aide des commandes de gestion des paramètres d'intégration avec Sandbox, vous pouvez gérer les certificats utilisés pour se connecter aux serveurs qui assurent l'interaction avec Sandbox.

Paramètres d'intégration avec Sandbox

Le tableau ci-dessous décrit tous les paramètres disponibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Intégration avec Sandbox (`Standalone_Sandbox`).

Comment configurer les paramètres d'intégration avec Sandbox

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

Paramètre	Description	Valeur
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. Si la vérification du certificat client est activée du côté serveur Sandbox, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Sandbox*.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur en secondes.	Valeur par défaut : `10`.
`SendingMode`	Mode d'envoi du fichier pour analyse à Sandbox.	`AutoOnly` (valeur par défaut) : envoi automatiquement des fichiers pour analyse dès qu'ils sont consultés. `Manual` : envoi manuel des fichiers pour analyse. `AutoAndManual` : envoi des fichiers à analyser, que ce soit automatique ou manuel.
`QuarantineFile`	Place un fichier en quarantaine lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : en cas de menace détectée, supprimer le fichier original et mettre la copie en quarantaine. `No` : ne pas placer le fichier en quarantaine en cas de menace détectée.
`ScanCriticalAreas`	Exécution de l'analyse des zones critiques en cas de menace détectée.	`Yes` (valeur par défaut) : lorsqu'une menace est détectée, effectuer une analyse des zones critiques. `No` : ne pas lancer d'analyse des zones critiques lorsqu'une menace est détectée.
`CreateIocScanTask`	Créer une tâche d'analyse IOC lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : créer une tâche d'analyse IOC lorsqu'une menace est détectée. `No` : ne pas créer de tâche d'analyse IOC lorsqu'une menace est détectée.
`QuarantineFileOnIocDetected`	Mise en quarantaine d'un objet lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, supprimer l'objet original et mettre en quarantaine la copie de l'objet. `No` : ne pas mettre l'objet en quarantaine lorsqu'un indicateur de compromission est détecté.
`ScanCriticalAreasOnIocDetected`	Exécution de l'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, exécuter une analyse des zones critiques. `No` : ne pas exécuter d'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.
`Drives`	Domaines de recherche d'indicateurs de compromission.	`Critical` (valeur par défaut) : vérifier les fichiers dans les répertoires utilisateur et système. `System` : analyser tous les fichiers du système de fichiers racine.
`ScheduleMode`	Mode de lancement de la tâche d'analyse IOC.	`Manually` (valeur par défaut) : exécuter manuellement la tâche d'analyse IOC. `AfterTreatDetected` : exécuter la tâche d'analyse IOC après la détection d'une menace.
La section **[Servers.item_#]** contient les paramètres du serveur Sandbox.		
`Address`	Adresse du serveur. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.

Paramètre	Description	Valeur
`Port`	Port de connexion au serveur.	Valeur par défaut : `443`.
La section **[SandboxTransferSettings]** contient les paramètres de transfert des fichiers à analyser dans Sandbox.		
`SandboxQueue`	Taille maximale du répertoire de stockage de la file d'attente des demandes d'analyse en mégaoctets.	Valeur par défaut : `1024`.

Gestion des certificats pour la connexion au serveur Sandbox

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez gérer, à l'aide de commandes, les certificats utilisés pour les connexions aux serveurs OSMP ou aux serveurs Central Node responsables de l'interaction avec Sandbox (ci-après également appelés serveurs Sandbox). Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer un certificat client ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

où `<file>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   où `<file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Saisissez le mot de passe du cryptocontainer

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur Sandbox si la vérification du certificat client est activée dans les paramètres du serveur Sandbox et si, dans les paramètres de la tâche *Intégration avec Sandbox*, `UseClientCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat, exécutez la commande suivante :

- pour le certificat du serveur :

```
kesl-control [-X] --query-sandbox-server-certificate
```

- pour le certificat client :

```
kesl-control [-X] --query-sandbox-client-certificate
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum

À partir de la ligne de commande, vous pouvez activer ou désactiver le module EDR Optimum à l'aide du paramètre `UseEdrOptimum` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Pour activer le module EDR Optimum à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Pour désactiver le module EDR Optimum à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Configuration de l'intégration de Kaspersky Managed Detection and Response

Sur la ligne de commande, vous pouvez :

- Activer ou désactiver le module MDR.
- Télécharger et supprimer le fichier MDR BLOB, qui contient des informations sur la licence Kaspersky Managed Detection and Response.

  Si vous utilisez une clé de licence pour activer le module MDR, vous n'avez pas besoin de télécharger le fichier BLOB MDR.

il est recommander de configurer l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response dans la Console d'administration ou dans Web Console.

Vous pouvez activer ou désactiver le module MDR à l'aide du paramètre `UseMDR` des paramètres généraux de l'application. Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseMDR` peut prendre les valeurs suivantes :

- `Yes` : activer le module MDR.
- `No` : désactiver le module MDR.

Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, un message d'erreur s'affiche et le module MDR n'est pas activé. Pour activer le module MDR, vous devez activer l'utilisation de KSN en mode avancé.

Vous pouvez charger et supprimer le fichier BLOB à l'aide des commandes de gestion des clés de licence. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR.

Pour charger le fichier BLOB, exécutez la commande suivante :

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

Pour supprimer le fichier BLOB, exécutez la commande suivante :

```
kesl-control --remove-mdr-blob
```

Après avoir activé l'intégration, la tâche de service `Mdr_Autostart_Scan` est créée dans l'application avec un mode de lancement une fois par jour.

Administration de l'isolation réseau des appareils

Lors de l'intégration avec les solutions Detection and Response, vous pouvez effectuer les actions suivantes à l'aide de la ligne de commande :

- vérifier l'état d'isolement réseau d'un appareil et afficher la liste des exclusions d'isolement du réseau ;
- désactiver l'isolement réseau de l'appareil.

Pour désactiver l'isolement réseau d'un appareil, exécutez la commande suivante :

```
kesl-control [-R] --isolation-off
```

Pour vérifier l'état de l'isolement du réseau et afficher la liste des exclusions de l'isolement du réseau, exécutez la commande suivante :

```
kesl-control [-R] --isolation-stat
```

Pour l'isolement du réseau, l'un des états suivants s'affiche :

- *Isolement du réseau activé*.
- *Isolation réseau désactivée*.

Configuration des paramètres de la quarantaine

Dans la ligne de commande, vous pouvez configurer les paramètres de la quarantaine à l'aide des paramètres `QuarantineSizeLimit`, `QuarantineFillingNotification` et `QuarantineBackupFolder` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Paramètres de quarantaine

Paramètre	Description	Valeur
`QuarantineFillingNotification`	Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Pour désactiver la génération des événements sur la quarantaine complète, spécifiez la valeur 0.	0 – 100 0 : la génération des événements concernant le remplissage de la quarantaine est désactivée. Valeur par défaut : 90.

Paramètre	Description	Valeur
`QuarantineSizeLimit`	Volume maximal de la quarantaine (en mégaoctets). Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime les fichiers les plus anciens. Pour supprimer la limite de taille de la quarantaine, saisissez la valeur 0.	0 – 4000 0 : la taille de la quarantaine est illimitée. La valeur par défaut est de 200 si l'application est utilisée en mode standard ou en mode EDR Agent, et de 100 si l'application est utilisée en mode Light Agent.
`QuarantineBackupFolder`	Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine. Vous pouvez définir un répertoire autre que celui défini par défaut. Les répertoires de n'importe quel appareil peuvent être utilisés comme répertoire pour stocker des objets de sauvegarde et de quarantaine. Il est déconseillé de désigner des répertoires qui se trouvent sur des appareils à distance, par exemple des répertoires montés via les protocoles Samba et NFS. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : /var/opt/kaspersky/kesl/common/objects-backup/ L'accès au répertoire par défaut requiert les privilèges root.

Travailler avec des fichiers de quarantaine dans la ligne de commande

Lorsqu'il est intégré avec les solutions Detection and Response, vous pouvez effectuer les actions suivantes à l'aide des commandes de gestion de la quarantaine :

- Placer les fichiers en quarantaine (uniquement lorsqu'ils sont intégrés à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response).
- Afficher des informations sur les fichiers mis en quarantaine.
- Supprimer tous les fichiers spécifiés ou uniquement ceux spécifiés de la quarantaine.
- Restauration d'un fichier depuis la quarantaine.

La restauration d'objets infectés peut infecter l'appareil.

Mettre un fichier en quarantaine

Pour mettre un fichier en quarantaine, exécutez la commande suivante :

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

où :

- `<path to the file>` est le chemin d'accès au fichier que vous souhaitez mettre en quarantaine.
- `--md5` : somme de hachage MD5 du fichier que vous souhaitez mettre en quarantaine ;
- `--sha256` : somme de hachage SHA256 du fichier que vous souhaitez mettre en quarantaine ;

- `--save-original-file` : ne pas supprimer le fichier d'origine. Si vous ne spécifiez pas cette clé, le fichier d'origine sera supprimé.

  Le fichier d'origine est supprimé uniquement si le compte utilisateur dispose de l'autorisation de supprimer des objets. Si les droits sont insuffisants, un message d'erreur concernant la suppression du fichier s'affiche.

Vous ne pouvez utiliser cette commande que lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response.

Afficher des informations sur les fichiers mis en quarantaine

Pour afficher des informations sur les fichiers mis en quarantaine, exécutez la commande suivante :

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

où :

- `<filter conditions>` indique une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'`, combinées à l'aide de l'opérateur logique `and` afin de limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtrage, l'application affichera des informations sur tous les fichiers mis en quarantaine.

- `<number of files>` est le nombre de fichiers les plus récemment mis en quarantaine que vous souhaitez afficher. Si vous ne spécifiez pas la clé `-n`, les 30 derniers fichiers seront affichés. Pour afficher tous les fichiers, saisissez la valeur 0.

- `--json` : afficher les données au format JSON.

La ligne `ObjectId` affichera l'identifiant numérique que l'application a attribué au fichier lors de sa mise en quarantaine. Cet identifiant est utilisé pour effectuer des actions sur le fichier, telles que la restauration ou la suppression du fichier de la quarantaine.

Restaurer les fichiers depuis la quarantaine

Pour restaurer un fichier mis en quarantaine avec son nom d'origine vers son emplacement d'origine, exécutez la commande suivante :

```
kesl-control -Q --restore <object identifier>
```

où `<object identifier>` est l'identifiant numérique que l'application a attribué au fichier lors de sa mise en quarantaine.

Pour restaurer un fichier avec un nouveau nom de la quarantaine vers le répertoire spécifié, exécutez la commande suivante :

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

où --file `<path to the file>` est le nouveau nom du fichier et le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier.

Vous ne pouvez restaurer un fichier de la quarantaine vers un autre répertoire que si votre compte dispose des droits root. S'il n'y a pas assez de privilèges, le fichier ne peut être restauré qu'à son emplacement d'origine.

Sur les appareils exécutant le système d'exploitation Astra Linux, en mode environnement logiciel fermé, vous ne pouvez restaurer un fichier que sous le compte sous lequel il a été placé dans la sauvegarde. Lors de la restauration d'un fichier, l'application crée un répertoire avec l'étiquette MAC 3 (indicateur cnnr).

Mettre un fichier en quarantaine

Pour supprimer les fichiers sélectionnés de la quarantaine, exécutez la commande suivante :

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

où `<filter conditions>` spécifie une ou plusieurs expressions logiques au format <field><comparison operation>'<value>', combinées à l'aide de l'opérateur logique « and » afin de restreindre les résultats de la requête.

```
Exemple de suppression des fichiers qui contiennent « test » dans leur nom ou leur chemin
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

Pour supprimer tous les fichiers de la quarantaine, exécutez la commande suivante :

```
kesl-control -Q --mass-remove
```

Trouver des indicateurs de compromission

Vous pouvez rechercher des indicateurs de compromission à l'aide de la tâche d'analyse IOC dans la ligne de commande uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response (on-premises) ou Kaspersky Endpoint Detection and Response (KATA), l'Analyse IOC est exécutée du côté de la solution Detection and Response correspondante.

Pour créer, configurer et exécuter la tâche Analyse IOC dans la ligne de commande, exécutez la commande suivante :

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

où :

- `--path <path to the directory or file>` est le chemin d'accès au fichier IOC ou au répertoire contenant des fichiers IOC portant l'extension .IOC ou .XML, à utiliser pour effectuer l'analyse.

  Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces. Vous pouvez également spécifier les deux types de chemins (fichier et répertoire).

- `--process` : activation de l'analyse des processus en cours d'exécution sur l'appareil.

  Arguments possibles :

  - `on` : activer l'analyse des processus en cours d'exécution sur l'appareil (valeur par défaut).
  - `off` : désactiver l'analyse des processus en cours d'exécution sur l'appareil.

  Si vous n'indiquez pas la clé `--process`, l'application effectue une analyse de processus uniquement si le fichier IOC utilisé contient les données de processus (`ProcessItem`).

- `--hint <regular expression>` est l'expression régulière qui correspond au chemin complet du fichier (`FileItem`) ou du fichier exécutable du processus (`ProcessItem`) à analyser.

  Vous pouvez utiliser les éléments d'expressions régulières suivants :

  - métacaractères : `. ^ $ |`
  - classes de caractères : chiffre, alpha, inférieur, supérieur, cntrl
  - quantificateurs : `* + ? {n} {n,} {n, m}`
  - négation : `[^a-c]`
  - caractères d'échappement : `\a \e \f`, `\n \r \t \v \b`

- `--arpentry` : activation de l'analyse des enregistrements dans la tableau ARP (`ArpEntryItem`).

  Arguments possibles :

  - `on` : activer l'analyse des enregistrements dans le tableau ARP (valeur par défaut).
  - `off` : désactiver l'analyse des enregistrements dans le tableau ARP.

  Si vous n'indiquez pas la clé `--arpentry`, l'application analyse la tableau ARP uniquement si le fichier IOC utilisé contient les données de la table (`ArpEntryItem`).

  `--ports` : activation de l'analyse des ports ouverts pour la connexion.

Arguments possibles :

- `on` : activer l'analyse des ports ouverts pour les connexions et vérifier les connexions actives sur l'appareil (valeur par défaut).
- `off` : désactiver l'analyse des ports ouverts pour les connexions et ne pas vérifier les connexions actives sur l'appareil.

Si vous n'indiquez pas la clé `--ports`, l'application effectue une analyse de ports uniquement si le fichier IOC utilisé contient les données de ports (`PortItem`).

- `--system` : activation de l'analyse de l'environnement système.

  Arguments possibles :

  - `on` : activation de l'analyse de l'environnement système (valeur par défaut).
  - `off` : désactivation de l'analyse de l'environnement système.

  Si vous n'indiquez pas la clé `--system`, l'application effectue une analyse de l'environnement système uniquement si les informations sur l'environnement système (`SystemInfoItem`) sont spécifiées dans le fichier IOC utilisé.

- `--files` : activation de l'analyse des fichiers.

  Arguments possibles :

  - `on` : activation de l'analyse des fichiers (valeur par défaut).
  - `off` : désactivation de l'analyse des fichiers.

  Si vous n'indiquez pas la clé `--files`, l'application effectue une analyse de fichiers uniquement si le fichier IOC utilisé contient les données de fichiers (`FileItem`).

- `--drives` : zones à analyser.

  Arguments possibles :

  - `all` : analyser toutes les zones de fichiers disponibles.
  - `system` : analyser tous les fichiers du système de fichiers racine.
  - `critical` : analyser les fichiers dans les répertoires utilisateur et système (valeur par défaut).
  - `custom` : analyser uniquement les fichiers dans les zones que vous spécifiez.

  Si vous ne spécifiez pas la clé `--drives`, l'application analyse les fichiers dans les répertoires utilisateur et système.

- `--excludes <list of exclusions>` est la liste des chemins exclus de l'analyse.

  Les exclusions spécifiées par cette clé sont globales et s'appliquent quel que soit le type de zone ou de liste de répertoires. Ces exclusions ont la priorité sur les autres options de ligne de commande, notamment `--hint` et `--scope`.

Les exclusions sont spécifiées sous forme de chemins, mais ne peuvent pas contenir des éléments récursifs ni de caractères de masque (par exemple, *).

Si vous ne spécifiez pas la clé `--excludes`, l'analyse est effectuée sans exclusion.

Vous pouvez spécifier plusieurs exclusions, séparées par des espaces.

- `--scope <list of directories>` est la liste des répertoires supplémentaires à analyser.

  Cette option est obligatoire si vous avez spécifié l'argument `--drives` pour l'option `custom`.

- `--action` : action effectuée lorsque des indicateurs de compromission sont détectés.

  Arguments possibles :

  - `Skip` : l'application n'effectuera aucune action avec l'objet détecté, mais les informations le concernant seront enregistrées dans les résultats de la tâche (valeur par défaut).
  - `QuarantineFile` : l'application mettra en quarantaine l'objet détecté.
  - `IsolateHost` : l'application isole du réseau l'appareil sur lequel l'objet est détecté.
  - `ScanCriticalAreas` : l'application exécutera l'analyse des zones critiques.

    Zones critiques analysées par Kaspersky Endpoint Security

    - /lib/systemd
    - /lib/udev
    - /lib/dbus-1.0
    - /usr/local/lib/systemd/user
    - /usr/share/dbus-1
    - /usr/share/gdm/autostart
    - /usr/share/gnome/autostart
    - /var/spool/at
    - /var/spool/at/spool
    - /var/spool/anacron
    - /var/spool/cron
    - /boot
    - /bin
    - /sbin

- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Vous pouvez spécifier plusieurs actions séparées par des espaces.

> Si vous avez spécifié l'argument `Skip`, vous n'avez pas besoin d'ajouter d'autres arguments. L'argument `Skip` ne peut être utilisé que de manière indépendante.

Gestion de la prévention de l'exécution

La prévention de l'exécution permet de gérer l'exécution de fichiers exécutables et de scripts, ainsi que d'ouvrir des fichiers au format Office. La Prévention de l'exécution gère l'accès de l'utilisateur aux fichiers à l'aide de règles de prévention de l'exécution.

La Prévention du lancement des objets comprend les tâches suivantes :

- *Prévention de l'exécution des objets (EDR Expert (on-premises))*
- *Prévention de l'exécution des objets (EDR Expert (on-premises))*
- Prévention de l'exécution des objets (EDR Optimum) (*EDRO_Prevention*)

Par défaut, les tâches de *Prévention de l'exécution des objets* ne sont pas lancées. Si vous avez ajouté au moins une règle de prévention de l'exécution, l'application lance la tâche.

Pour afficher la liste des règles de prévention de l'exécution, exécutez la commande suivante :

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

où :

`--kata` : liste des règles de prévention de l'exécution du module EDR Expert (on-premises)

`--cxdr` : liste des règles de prévention de l'exécution du module EDR Expert (cloud)

`--edro` : liste des règles de prévention de l'exécution du module EDR Optimum

Configuration de l'intégration KUMA

À partir de la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Unified Monitoring and Analysis Platform* .

Par défaut, la tâche *Intégration avec Kaspersky Unified Monitoring and Analysis Platform* n'est pas lancée. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Unified Monitoring and Analysis Platform en modifiant les paramètres d'une tâche prédéfinie.

À l'aide des commandes de gestion des paramètres d'intégration avec Kaspersky Unified Monitoring and Analysis Platform, vous pouvez gérer les certificats utilisés pour se connecter aux serveurs KUMA.

Tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform

Le tableau décrit tous les paramètres disponibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform (`KUMA`).

Paramètres de la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform

Paramètre	Description	Valeur
`UseTls`	Activation ou désactivation de l'analyse du certificat du serveur pour sécuriser davantage la connexion au serveur KUMA.	`Yes` : utiliser le certificat pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser le certificat pour sécuriser la connexion au serveur KUMA.
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Si l'analyse du certificat client est activée du côté serveur KUMA, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KUMA en secondes.	Valeur par défaut : `5`.
La section **[Servers.item_#]** contient les paramètres du serveur KUMA.		

Paramètre	Description	Valeur
`ServerAddress`	Adresse du serveur KUMA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Si vous définissez `UseTls=Yes`, vous devez fournir le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat de votre licence KUMA.	Valeur par défaut : `127.0.0.1`.
`ServerPort`	Port de connexion au serveur KUMA.	Valeur par défaut : `443`.
`ServerProtocol`	Protocole pour se connecter au serveur KUMA.	`tcp` (valeur par défaut) : utiliser le protocole TCP pour la connexion au serveur KUMA. `HTTPWithCompression` : utiliser le protocole HTTP avec compression des événements pour se connecter au serveur KUMA. `udp` : utiliser le protocole UPD pour la connexion au serveur KUMA. Lorsque le protocole UDP est sélectionné, l'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge (les valeurs des paramètres `UseTls`, `UseClientCertificate` et `ConnectionTimeout` sont ignorées), et il n'y a aucun événement concernant la connexion au serveur KUMA.
La section **[KumaTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur KUMA.		
`EventTransferTimeMax`	Délai maximum en secondes pour l'envoi des événements au serveur KUMA.	Valeur par défaut : `30`.

Gestion des certificats pour la connexion au serveur KUMA

Lorsque le protocole UDP est sélectionné, l'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge.

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur KUMA. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer un certificat client ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

où `<path to the file>` est le chemin d'accès au fichier qui contient le certificat du serveur, au format DER ou PEM.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande:

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   où `<path to the file>` est le chemin d'accès au cryptocontainer (archive PFX) contenant le certificat client et la clé privée.

2. Saisissez le mot de passe du cryptocontainer

Le certificat client est utilisé pour assurer une protection supplémentaire de la connexion au serveur KUMA si la vérification du certificat client est activée dans les paramètres du serveur KUMA et si, dans les paramètres de la tâche *Intégration avec Kaspersky Unified Monitoring and Analysis Platform*, le paramètre `UseClientCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat, exécutez la commande suivante :

- pour le certificat du serveur :

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- pour le certificat client :

  ```
  kesl-control [-M] --query-kuma-client-certificate
  ```

  La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-M] --remove-kuma-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-M] --remove-kuma-client-certificate
```

Paramètres généraux

Dans la Console d'administration, vous pouvez gérer les paramètres généraux de l'application qui définissent le fonctionnement de l'application dans son ensemble et celui de ses fonctions individuelles, dans les propriétés de la stratégie (**Paramètres généraux**).

Paramètres généraux de l'application

Le tableau ci-dessous décrit les paramètres généraux de l'application qui régissent le fonctionnement de l'application dans son ensemble et celui de ses fonctions individuelles.

Paramètres généraux de l'application

Paramètre	Description	Valeurs
`SambaConfigPath`	Répertoire dans lequel se trouve le fichier de configuration Samba. Le fichier de configuration Samba est nécessaire pour garantir l'application des valeurs `AllShared` ou `Shared:SMB` du paramètre `Path`. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Le répertoire standard du fichier de configuration S indiqué par défaut. Valeur par défaut : /etc/samba/smb.conf.
`NfsExportPath`	Répertoire dans lequel se trouve le fichier de configuration NFS. Le fichier de configuration NFS est nécessaire pour garantir l'application des valeurs `AllShared` ou `Shared:NFS` du paramètre `Path`. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Le répertoire standard du fichier de configuration N indiqué par défaut. Valeur par défaut : /etc/exports.
`TraceFolder`	Répertoire dans lequel se trouvent les fichiers de traçage de l'application. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Valeur par défaut : /var/log/kaspersky/kesl. L'accès au répertoire des fichiers de trace par défa les privilèges root. Si vous indiquez un autre réperto assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce réperto (autorisations `700` ou `rwx--------`).

Paramètre	Description	Valeurs
`TraceLevel`	Activer le traçage des applications et le niveau de détails des fichiers de traçage. Ce paramètre active uniquement la génération de fichiers de traçage de l'application. Pour générer des fichiers de traçage pour l'interface graphique et l'utilitaire de ligne de commande kesl-control, vous devez définir la variable d'environnement LFS_ENABLE_ALL_COMPONENTS_LOGGING.	`Detailed` – crée un fichier de traçage détaillé de l `MediumDetailed` – crée un fichier de traçage de l' contenant des messages d'information et des mes d'erreur. `NotDetailed` – crée un fichier de traçage de l'app contenant des messages d'erreur. `None` (valeur par défaut) – ne crée pas de fichier d l'application.
`TraceMaxFileCount`	Spécifie le nombre maximal de fichiers de traçage d'application. Le relancement de l'application est nécessaire après la modification de ce paramètre.	1 à 10000 Valeur par défaut : 10.
`TraceMaxFileSize`	Définit la taille maximale d'un fichier de trace de l'application (en mégaoctets). Le relancement de l'application est nécessaire après la modification de ce paramètre.	1 à 1000 Valeur par défaut : 500.
`WdTraceLevel`	Activer le traçage du serveur Watchdog et configurer le niveau de détail des fichiers de traçage.	`Detailed` – crée un fichier de traçage détaillé du s Watchdog. `MediumDetailed` – crée un fichier de traçage du s Watchdog contenant des messages d'information messages d'erreur. `NotDetailed` – crée un fichier de traçage du serv Watchdog contenant des messages d'erreur. `None` – Ne pas générer de fichier de traçage du se Watchdog. `Product` (valeur par défaut) – Définir une valeur ég valeur `TraceLevel`.
`BlockFilesGreaterMaxFileNamePath`	Blocage de l'accès aux fichiers dont la longueur du chemin d'accès complet dépasse la valeur du paramètre définie (en octets). Si la longueur du chemin complet d'accès au fichier analysé excède la valeur de ce paramètre, les tâches d'analyse ignorent ce fichier lors de l'analyse. Ce paramètre s'applique uniquement aux systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify. Après avoir modifié la valeur de ce paramètre, relancez la tâche Protection contre les fichiers malicieux.	4096 à 33 554 432 Valeur par défaut : 16384.
`DetectOtherObjects`	Activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.	`Yes` : activer la détection des applications légitimes intrus peuvent utiliser pour endommager les appare données. `No` (valeur par défaut) : désactiver la détection des applications légitimes que les intrus peuvent utilise endommager les appareils ou les données.

Paramètre	Description	Valeurs
`NamespaceMonitoring`	Activation de l'analyse des espaces de noms et des conteneurs. L'application ne vérifie pas les espaces de noms et les conteneurs à moins que les modules permettant de travailler avec les conteneurs et les espaces de noms ne soient installés sur le système d'exploitation.	`Yes` (valeur par défaut) active l'analyse des espace et des conteneurs. `No` désactive l'analyse des espaces de noms et des conteneurs.
`FileBlockDuringScan`	Activation du mode d'interception pour les opérations sur les fichiers avec blocage de l'accès aux fichiers pendant l'analyse. Le mode d'interception des opérations sur les fichiers affecte les modules Protection contre les fichiers malicieux et Contrôle des appareils, l'action Prévention de l'exécution des objets et la tâche Analyse des disques amovibles.	`Yes` (valeur par défaut) — Bloquer l'accès aux fichie la durée de l'analyse. `No` : ne pas bloquer l'accès aux fichiers lors de l'ana à n'importe quel fichier est autorisé, la vérification e effectuée en mode asynchrone. Cependant, les mo Protection contre les fichiers malicieux, Contrôle d et Prévention de l'exécution, ainsi que la tâche Anal disques amovibles, fonctionnent en mode Informat soit le mode de fonctionnement sélectionné. Ce m d'interception des opérations sur les fichiers a moir sur les performances du système, mais les menace dans les fichiers ne seront alors ni désinfectées ni s Cela peut se produire si, pendant l'analyse, le proce associé à ce fichier parvient à renommer le fichier a l'application puisse prendre une décision sur l'état d Vous pouvez exécuter la tâche Analyse des logiciel malveillants pour traiter ces menaces ultérieuremer
`UseKSN`	Configuration de l'utilisation de Kaspersky Security Network dans l'application.	`Basic` : activer l'utilisation de Kaspersky Security N mode standard. `Extended` : activer l'utilisation de Kaspersky Secur en mode avancé. `No` (valeur par défaut) : ne pas utiliser Kaspersky Se Network.
`CloudMode`	Activation du mode cloud de l'application. Le mode Cloud est disponible si l'utilisation de KSN est activée. Si vous prévoyez d'utiliser le mode cloud, assurez-vous que KSN est disponible sur votre appareil. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`Yes` (valeur par défaut) — Activer le mode de fonct dans lequel Kaspersky Endpoint Security utilise une allégée des bases de données des applications mal `No` (valeur par défaut) : utiliser la version complète de données des applications malveillantes. Le mode Cloud est automatiquement désactivé l'utilisation de KSN est désactivée.
`UseMDR`	Activation du module Managed Detection and Response pour l'intégration avec Kaspersky Managed Detection and Response. Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, un message d'erreur s'affiche et le module MDR n'est pas activé. Pour activer le module MDR, vous devez activer l'utilisation de KSN en mode avancé. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : activer le module Managed Detection and Re `No` (valeur par défaut) : désactiver le module Manag Detection and Response.

Paramètre	Description	Valeurs
`UseEdrOptimum`	Activation du module EDR Optimum pour l'intégration avec Kaspersky Endpoint Detection and Response Optimum. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : activer le module EDR Optimum. `No` (valeur par défaut) : désactiver le module EDR O
`UseProxy`	Activation de l'utilisation d'un serveur proxy par les modules de l'application Kaspersky Endpoint Security. Le serveur proxy peut être utilisé pour accéder aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites à l'aide du module Protection contre les menaces Internet. Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'utilisation d'un serveur proxy pour la connexion à Kaspersky Security Network, à la SVM et au Serveur d'intégration n'est pas prise en charge.	`Yes` : active l'utilisation d'un serveur proxy. `No` (valeur par défaut) : désactiver l'utilisation d'un s proxy.
`ProxyServer`	Adresse du serveur proxy à utiliser pour la connexion à Internet. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.	Adresse du serveur proxy dans l'un des formats sui • `[<connection protocol>://]<address o proxy server>:<port>`, si aucune authentifi n'est requise pour se connecter au serveur pro • `[<connection protocol>://][<user nam [<password>]@]<address of the proxy <port>`, si l'authentification est requise pour s au serveur proxy. Lorsque vous indiquez une ad saisissez-la entre crochets. La connexion à un serveur proxy via le protocole n'est pas prise en charge.
`ProxyBypass`	Liste des adresses pour lesquelles un serveur proxy n'est pas utilisé.	L'adresse est spécifiée au format `<address>[:<p` spécifier des adresses, vous pouvez utiliser des ma (symbole `*`) et des commentaires après le symbole
`ProxyBypassEdr`	Utiliser un serveur proxy lors de la connexion aux serveurs d'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises). Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` pour ne pas utiliser de serveur proxy lors de la aux serveurs d'intégration de Kaspersky Endpoint D and Response Expert (on-premises). `No` (valeur par défaut) pour utiliser un serveur proxy connexion aux serveurs d'intégration de Kaspersky Detection and Response Expert (on-premises).
`ProxyBypassNdr`	Utiliser un serveur proxy lors de la connexion aux Serveurs permettant l'intégration de Kaspersky Network Detection and Response (KATA). Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : ne pas utiliser de serveur proxy lors de la con serveurs assurant l'intégration avec Kaspersky Net Detection and Response (KATA). `No` (valeur par défaut) : utiliser un serveur proxy po connecter aux serveurs assurant l'intégration avec Network Detection and Response (KATA).

Paramètre	Description	Valeurs
`ProxyBypassSandbox`	Utiliser d'un serveur proxy lors de la connexion aux serveurs qui permettent l'interaction avec Sandbox. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : ne pas utiliser de serveur proxy lors de la con serveurs qui permettent l'interaction avec Sandbo `No` (valeur par défaut) : utiliser un serveur proxy lor connexion aux serveurs qui permettent l'interactio Sandbox.
`MaxEventsNumber`	Quantité maximale d'événements qui sera enregistrée dans l'application. Quand la quantité maximale d'événements définie est atteinte, l'application supprime les événements les plus anciens.	Valeur par défaut : 500 000. Si défini sur 0, les nouveaux événements ne sont pa enregistrés et les anciens événements seront supp
`LimitNumberOfScanFileTasks`	Nombre maximum de tâches d'analyse personnalisée qu'un utilisateur non privilégié peut exécuter simultanément sur un appareil. Ce paramètre ne limite pas la quantité de tâches que l'utilisateur doté des autorisations root ou du rôle kesladmin peut démarrer.	0 à 100000 0 : un utilisateur non privilégié ne peut pas lancer de d'analyse personnalisée. Valeur par défaut : 100.
`UseSyslog`	Activer la journalisation des événements de l'application dans syslog. L'accès à syslog requiert les privilèges root.	`Yes` : active l'enregistrement des événements dans `No` (valeur par défaut) : désactiver l'enregistrement événements dans syslog.
`EventsStoragePath`	Chemin vers le fichier principal de la base de données du journal des événements. L'accès à la base de données des événements par défaut requiert les privilèges root.	Valeur par défaut : `/var/opt/kaspersky/kesl/private/storage/`
`ExcludedMountPoint.item_#`	Point de montage que vous souhaitez exclure de la zone d'analyse. L'exclusion est appliquée dans le fonctionnement des modules Protection contre les fichiers malicieux, Protection contre le chiffrement, Surveillance du conteneur et dans la tâche Analyse des lecteurs amovibles, et est également configurée dans le fonctionnement des tâches d'analyse (types ODS et ContainerScan). Vous pouvez indiquer plusieurs points de montage à exclure d'une analyse. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`. Le paramètre `ExcludedMountPoint.item_#` n'est pas défini par défaut.	`AllRemoteMounted` : exclut de l'interception des o de fichiers tous les répertoires distants montés sur via les protocoles SMB et NFS. `Mounted:NFS` : exclut de l'interception des opérati fichiers tous les répertoires distants montés sur l'o le protocole NFS. `Mounted:SMB` : exclut de l'interception des opérati fichiers tous les répertoires distants montés sur l'o le protocole SMB. `Mounted:<file system type>` : exclut de l'interc opérations sur les fichiers tous les répertoires mon type de système de fichiers indiqué. `/mnt` — exclut les objets du point de montage /mn les sous-répertoires) de l'interception des opératio fichiers. Ce répertoire est utilisé comme point de m temporaire pour les disques amovibles. `<path that contains the /mnt/user*|/mnt/**/user_share>` : exclut de l'i des opérations sur les fichiers les objets situés dan de montage dont les noms contiennent le masque
`MemScanExcludedProgramPath.item_#`	Exclusion de la mémoire d'un processus de l'analyse L'application n'analysera pas la mémoire du processus spécifié.	`<full path to process>` — Exclure de l'analyse du répertoire indiqué. Vous pouvez utiliser des mas spécifier le chemin.
`PowerSaveMode`	Annulez l'exécution des tâches planifiées sur un appareil fonctionnant sur batterie.	`Yes` (valeur par défaut) : ignorer l'exécution des tâc planifiées lorsque l'appareil fonctionne sur batterie. `No` : exécuter les tâches selon un calendrier, quelle source d'alimentation à laquelle l'appareil est conne ou batterie).

Paramètre	Description	Valeurs
`UseOnDemandCPULimit`	Active les limites d'utilisation du processeur pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan*.	`Yes` active la limitation de la consommation des res processeur pour les tâches de type *ODS*, *Containe* *InventoryScan*. `No` (valeur par défaut) : désactiver la limite de cons des ressources CPU pour les tâches.
`OnDemandCPULimit`	Utilisation maximale de tous les cœurs du processeur (en pourcentage) lors de l'exécution des tâches de type *ODS*, *ContainerScan* et *InventoryScan*.	Un entier compris entre 10 et 100. Valeur par défaut : 100.
`BackupSizeLimit`	Volume maximal de la sauvegarde (Mo). Quand la taille de la sauvegarde atteint la valeur maximale définie, l'application supprime les objets les plus anciens. Pour supprimer la limite sur la taille de la sauvegarde, spécifiez la valeur 0.	0 – 4000 0 : la taille de la sauvegarde est illimitée. Valeur par défaut : 0.
`BackupDaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Après une durée spécifiée, l'application supprime les fichiers de sauvegarde les plus anciens. Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.	0 – 10000 0 : la durée de conservation des objets dans la sauv n'est pas limitée. Valeur par défaut : 30.
`QuarantineSizeLimit`	Volume maximal de la quarantaine (en mégaoctets). Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime les fichiers les plus anciens. Pour supprimer la limite de taille de la quarantaine, saisissez la valeur 0. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	0 – 999999 0 : la taille de la quarantaine est illimitée. La valeur par défaut est 200 si l'application est utili mode standard, et 100 si l'application est utilisée en Agent.
`QuarantineFillingNotification`	Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Pour désactiver la génération des événements sur la quarantaine complète, spécifiez la valeur 0. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	0 – 100 0 : la génération des événements concernant le rem la quarantaine est désactivée. Valeur par défaut : 90.
`QuarantineBackupFolder`	Chemin d'accès au répertoire où sont stockés les copies de sauvegarde des fichiers et les fichiers mis en quarantaine. Vous pouvez modifier le répertoire par défaut. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus. Le paramètre `BackupFolder` est utilisé.	Valeur par défaut : `/var/opt/kaspersky/kesl/common/objects-b` L'accès au répertoire par défaut requiert les priv root.

Paramètre	Description	Valeurs
`BackupFolder`	Chemin d'accès au répertoire de la copie de sauvegarde. Vous pouvez modifier le répertoire par défaut. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : `/var/opt/kaspersky/kesl/common/objects-b` L'accès au répertoire de la sauvegarde par défau requiert les privilèges root.
`ShowPopUpNotifications`	Activation de l'affichage des notifications contextuelles dans l'interface utilisateur graphique.	`Yes` (par défaut) : afficher les notifications context l'interface utilisateur graphique. `No` : ne pas afficher les notifications contextuelles l'interface utilisateur graphique.
`InterceptorMode`	Le mécanisme d'interception des événements système utilisé par l'application Kaspersky Endpoint Security dans son travail. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`UseFanotify` (valeur par défaut) : utiliser la techno fanotify pour intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module mis à jour pour intercepter les événements système
`InterceptorFallbackStrategy`	L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`FallbackToFanotify` (valeur par défaut) : passer l'utilisation de la technologie fanotify pour intercep événements système. `FallbackToLimitedMode` : ne pas utiliser l'interce événements système. Si l'application n'utilise pas l'i des événements système, l'analyse des fichiers en n'est pas effectuée, et le niveau de protection de l'a réduit.
`InterceptorApplyStrategy`	Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`RestartServiceAutomatically` : redémarrer automatiquement l'application pour exécuter le mo noyau à actualiser. Nous vous recommandons d'util paramètre. `RestartServiceManually` (valeur par défaut) : ex module de noyau mis à jour après le redémarrage m l'application par l'utilisateur.
`SystemEventsTransmission`	Activation de la transmission d'informations sur les événements des applications tierces (qui ne sont pas des solutions Kaspersky). Si ce paramètre est activé, en plus de ses propres événements, Kaspersky Endpoint Security envoie également les événements systemd-journald des applications tierces au journal des événements de l'application. Les privilèges root sont requis pour accéder à systemd-journald.	`Yes` active la transmission d'informations sur les év systemd-journald des applications tierces au journa événements de l'application. `No` (par défaut) désactive la transmission d'informa événements systemd-journald des applications tier journal des événements de l'application.

Paramètre	Description	Valeurs
`UrgentUpdateRestartEnabled`	Redémarrer automatiquement l'application à la réception de mises à jour critiques.	`Yes` pour redémarrer automatiquement l'applicatio réception de mises à jour critiques. `No` (valeur par défaut) pour ne pas redémarrer l'app réception de mises à jour critiques. Si des mises à jour critiques sont reçues lors de la p mise à jour des bases de données et des modules d heures suivant l'installation de l'application, celle-ci automatiquement, quelle que soit la valeur du paran `UrgentUpdateRestartEnabled`.
`CoreDumps`	Permettre la création d'un fichier de vidage lorsque l'application plante.	`Yes` pour créer un fichier de vidage en cas de plant l'application. `No` (valeur par défaut) pour ne pas créer de fichier cas de plantage de l'application.
`CoreDumpsPath`	Chemin d'accès au répertoire où sont stockés les fichiers de vidage.	Valeur par défaut : `/var/opt/kaspersky/kesl/common/dumps` L'accès au répertoire de stockage des fichiers d défini par défaut requiert les autorisations root.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Planification de la tâche

Le tableau ci-dessous décrit les paramètres de planification des tâches que vous pouvez gérer pour toutes les tâches de l'application.

Paramètres de la programmation du lancement d'une tâche

Paramètre	Description
`RuleType`	Planifier l'exécution de la tâche. • `Once` : exécuter la tâche une fois. • `Monthly` : exécuter la tâche chaque mois, le jour et l'heure spécifiés. • `Weekly` : exécuter la tâche chaque semaine, le jour et l'heure spécifiés. • `Daily` : exécuter la tâche régulièrement, avec un intervalle spécifié en jours. • `Hourly` : exécuter la tâche régulièrement, à un intervalle spécifié en heures, à partir de la date et de l'heure spécifiées. • `Minutely` : exécuter la tâche régulièrement, à un intervalle spécifié en minutes, à partir de l'heure spécifiée. • `Manual` : lance la tâche manuellement. • `PS` : lance la tâche après le lancement de l'application. • `BR` : lancement de la tâche après la mise à jour des bases de données de l'application.
`StartTime`	La date et l'heure du lancement de la tâche. Le format de ce paramètre dépend de `RuleType`. Valeurs possibles : • `<year>` : 1970 à 2099 • `<month>` : JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>` : 1 à 31 • `<day of the week>` : Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>` : 0 à 23 • `<mm>` : 0 à 59 • `<ss>` : 0 à 59 • `<interval between runs (in days)>` : 0 à 364 • `<interval between runs (in hours)>` : 0 à 23 • `<interval between runs (in minutes)>` : 0 à 59
`RandomInterval`	Exécutez la tâche sur les ordinateurs de manière aléatoire dans un intervalle de temps donné (de 0 à la valeur spécifiée). Cela évite le lancement simultané de plusieurs tâches. Valeur par défaut : 99 minutes. Valeurs possibles : 0 à 999.
`RunMissedStartRules`	Lancement d'une tâche ignorée après le lancement de l'application. • `Yes` (valeur par défaut) signifie que l'exécution d'une tâche non exécutée est activée. Si l'application est arrêtée ou si l'ordinateur est éteint alors qu'une tâche planifiée est en cours d'exécution, Kaspersky Endpoint Security lance cette tâche immédiatement après le démarrage de l'application. Cela vous permet de vous assurer que les tâches critiques ne sont jamais omises. • `No` signifie que l'exécution d'une tâche non exécutée est désactivée. Si l'application est arrêtée ou si l'ordinateur est éteint alors qu'une tâche planifiée est en cours d'exécution, l'application ignore cette tâche. Cela permet d'éviter une surcharge lors du lancement de l'application.
`UseWorkingTimeout`	Arrêt de la tâche lorsque la durée maximale d'exécution de la tâche spécifiée par le paramètre `WorkingTimeout` est atteinte. La tâche sera arrêtée même si elle n'est pas terminée. Le prochain lancement de la tâche sera effectué comme prévu. • `Yes` : arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte. • `No` (valeur par défaut) : ne pas arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte.
`WorkingTimeout`	Le temps maximum d'exécution de la tâche (en minutes), après lequel l'application arrête l'exécution de la tâche, si la valeur du paramètre `UseWorkingTimeout=Yes`. Valeur par défaut : 120 minutes. Valeurs possibles : 1 à 999.

Configuration du serveur proxy

Dans la ligne de commande, vous pouvez configurer la manière dont les modules de l'application utilisent un serveur proxy à l'aide des paramètres `UseProxy`, `ProxyServer`, `ProxyBypass`, `ProxyBypassEdr`, `ProxyBypassNdr` et `ProxyBypassSandbox` des paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseProxy` peut prendre les valeurs suivantes :

- `Yes` active l'utilisation d'un serveur proxy.
- `No` désactive le serveur proxy.

Le paramètre ProxyServer permet de spécifier les paramètres du serveur proxy au format `<connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>`, où :

- `<user>` est le nom d'utilisateur utilisé pour l'authentification sur le serveur proxy.
- `<password>` est le mot de passe utilisateur utilisé pour l'authentification sur le serveur proxy.
- `<proxy server address>` est l'adresse IP ou le nom de domaine du serveur proxy.
- `<port number>` est le numéro de port du serveur proxy.

La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.

Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.

Le paramètre `ProxyBypass` vous permet de spécifier une liste d'adresses auxquelles un serveur proxy ne sera pas utilisé pour se connecter. L'adresse est spécifiée au format `<address>[:<port number>]`. Pour spécifier des adresses, vous pouvez utiliser des masques (symboles `*`) et des commentaires (après le symbole \).

Les paramètres suivants vous permettent de configurer l'utilisation d'un serveur proxy par les modules EDR Expert (on-premises), NDR (KATA) et Sandbox, qui assurent l'intégration avec les solutions Detection and Response :

- Le paramètre `ProxyBypassEdr` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion aux serveurs qui assurent l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA).
- le paramètre `ProxyBypassNdr` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion à des serveurs qui assurent l'intégration avec Kaspersky Network Detection and Response (KATA) ;
- le paramètre `ProxyBypassSandbox` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion aux serveurs qui fournissent une interaction avec Sandbox.

Les paramètres peuvent prendre les valeurs suivantes :

- `Yes` active l'utilisation d'un serveur proxy.
- `No` désactive le serveur proxy.

Configuration des paramètres de la sauvegarde

À partir de la ligne de commande, vous pouvez configurer les paramètres de la sauvegarde à l'aide des paramètres `BackupDaysToLive, BackupSizeLimit` et `QuarantineBackupFolder` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Paramètres de sauvegarde

Paramètre	Description	Valeur
`BackupDaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Après une durée spécifiée, l'application supprime les fichiers de sauvegarde les plus anciens. Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.	0 – 10000 0 : la durée de conservation des objets dans la sauvegarde n'est pas limitée. Valeur par défaut : 30.
`BackupSizeLimit`	Volume maximal de la sauvegarde (Mo). Quand la taille de la sauvegarde atteint la valeur maximale définie, l'application supprime les objets les plus anciens. Pour supprimer la limite sur la taille de la sauvegarde, spécifiez la valeur 0.	0 – 4000 0 : la taille de la sauvegarde est illimitée. Valeur par défaut : 0.
`QuarantineBackupFolder`	Chemin d'accès au répertoire où sont stockés les copies de sauvegarde des fichiers et les fichiers mis en quarantaine. Vous pouvez modifier le répertoire par défaut. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus. Le paramètre `BackupFolder` est utilisé.	Valeur par défaut : `/var/opt/kaspersky/kesl/common/objects-backup/` L'accès au répertoire par défaut requiert les privilèges root.
`BackupFolder`	Chemin d'accès au répertoire de la copie de sauvegarde. Vous pouvez modifier le répertoire par défaut. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : `/var/opt/kaspersky/kesl/common/objects-backup/` L'accès au répertoire de la sauvegarde par défaut requiert les privilèges root.

Paramètres d'analyse du trafic réseau

Paramètres d'analyse du trafic réseau

Paramètre	Description	Valeurs
`EncryptedConnectionsScan`	Active ou désactive l'analyse des connexions chiffrées. Pour le protocole FTP, l'analyse des connexions chiffrées est désactivée par défaut.	`Yes` (valeur par défaut) : active l'analyse des connexions chiffrées. `No` : désactive l'analyse des connexions chiffrées. L'application ne déchiffre pas le trafic chiffré.
`EncryptedConnectionsScanErrorAction`	Spécifie l'action à effectuer lorsqu'une erreur d'analyse de connexion chiffrée se produit sur un site Internet.	`AddToAutoExclusions` (valeur par défaut) : ajoute le domaine qui a entraîné l'erreur à la liste des domaines avec des erreurs d'analyse. L'application ne surveillera pas le trafic réseau chiffré lors de la visite de ce domaine. `Disconnect` : bloque la connexion réseau.
`CertificateVerificationPolicy`	Spécifie la façon dont Kaspersky Endpoint Security vérifie les certificats. Si un certificat est auto-signé, l'application n'effectue pas la vérification supplémentaire.	`FullCheck` (valeur par défaut) : l'application utilise Internet pour vérifier et télécharger les chaînes manquantes qui sont nécessaires pour vérifier un certificat. `LocalCheck` : l'application n'utilise pas Internet pour vérifier un certificat.

Paramètre	Description	Valeurs
`UntrustedCertificateAction`	L'action entreprise par l'application lorsqu'elle rencontre un certificat non vérifié.	`Allow` (valeur par défaut) : autorise la connexion réseau établie lors de la visite d'un domaine avec un certificat douteux. `Block` : bloque la connexion réseau établie lors de la visite d'un domaine avec un certificat douteux.
`ManageExclusions`	Utilisation d'exclusions lors de l'analyse du trafic chiffré.	`Yes` : ne pas analyser les sites spécifiés dans la section `[Exclusions.item_#]` (cf. ci-dessous). `No` (valeur par défaut) : analyse tous les sites Internet.
`MonitorNetworkPorts`	Manière dont Kaspersky Endpoint Security surveille les ports réseau.	`Selected` (valeur par défaut) : surveille uniquement les ports réseau spécifiés dans la section `[[NetworkPorts.item_#]` (voir ci-dessous). `All` : surveille tous les ports réseau. La spécification de cette valeur peut augmenter considérablement la charge d'un système d'exploitation.
`NetInterceptorMode`	Mode d'interception du trafic par l'application Kaspersky Endpoint Security. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`UseEBPF` : utiliser la technologie eBPF pour l'interception du trafic. `UseIPTables` (valeur par défaut) : utiliser l'utilitaire iptables pour intercepter le trafic. Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.
La section **[Exclusions.item_#]** contient les domaines à exclure de l'analyse. L'application n'analyse pas les connexions établies lors de la visite de domaines spécifiés.		
`DomainName`	Spécifie le nom de domaine.	Vous pouvez utiliser des masques pour spécifier le domaine.
La section **[IncomingEndpointsExclusions.item_#]** contient des exclusions pour le trafic entrant.		
`RemoteIp`	Une adresse IP de l'appareil distant, dont le trafic est exclu de l'interception.	
`DestinationPort`	Un port de l'appareil protégé, dont le trafic provenant des appareils distants est exclu de l'interception.	
La section **[OutgoingEndpointsExclusions.item_#]** contient des exclusions pour le trafic sortant.		
`RemoteIp`	Une adresse IP de l'appareil distant vers laquelle le trafic est exclu de l'interception.	
`DestinationPort`	Un port de l'appareil protégé vers lequel le trafic provenant d'un appareil protégé est exclu de l'interception.	
La section **[NetworkPorts.item_#]** contient les ports réseau que l'application doit surveiller.		
`PortName`	Description du port réseau.	
`Port`	Numéros de port réseau à surveiller par l'application.	`1` : `65535`. La valeur par défaut n'est pas définie.

Configuration des exclusions globales

À partir de la ligne de commande, vous pouvez configurer les exclusions de points de montage à l'aide du paramètre `ExcludedMountPoint.item_#` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `ExcludedMountPoint.item_#` peut prendre les valeurs suivantes :

- `AllRemoteMounted` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'appareil via les protocoles SMB et NFS.
- `Mounted:NFS` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole NFS.
- `Mounted:SMB` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole SMB.
- `Mounted:<file system type>` : exclut de l'interception des opérations sur les fichiers tous les répertoires montés avec le type de système de fichiers indiqué.
- `/mnt` — exclut les objets du point de montage /mnt (y compris les sous-répertoires) de l'interception des opérations sur les fichiers. Ce répertoire est utilisé comme point de montage temporaire pour les disques amovibles.
- `<path containing the mask /mnt/user* or /mnt/**/user_share>` : exclut de l'interception des opérations sur les fichiers les objets situés dans les points de montage dont les noms contiennent le masque indiqué.

> Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.

Vous pouvez spécifier plusieurs points de montage que vous souhaitez exclure de l'analyse.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Paramètres de la Protection par mot de passe

Vous pouvez octroyer ou révoquer les droits de gestion de l'application en modifiant les paramètres à l'aide des options de ligne de commande ou en modifiant un fichier de configuration.

Paramètres de la Protection par mot de passe

Paramètre	Description	Valeur
`StopProtection`	Désactivation des modules de protection.	`Yes` permet à l'utilisateur d'exécuter l'action. `No` interdit à l'utilisateur d'exécuter une action.
`StopSecurityControl`	Désactivation des modules de contrôle	
`StartProtection`	Activation des modules de protection	
`StartSecurityControl`	Activation des modules de contrôle	
`ApplicationSettings`	Configuration de l'application	
`ViewReports`	Consulter les rapports	
`RestoreFromBackup`	Restauration depuis la Sauvegarde	
`RemoveLicenseKey`	Suppression de la clé	
`AddLicense`	Ajout d'une clé	
`DisablePolicy`	Désactivation de la stratégie de Kaspersky Security Center	

Paramètres de l'application dans la Console d'administration

Vous utilisez une stratégie pour configurer Kaspersky Endpoint Security. Les informations détaillées sur les modules de l'application sont fournies dans les sous-sections correspondantes.

Mise à jour des bases de l'application

Dans la Console d'administration, vous pouvez mettre à jour les bases de données à l'aide de la tâche Update.

Vous pouvez créer et lancer des tâches de mise à jour définies par l'utilisateur. Vous pouvez gérer les paramètres de mise à jour en modifiant les paramètres des tâches.

Dans les propriétés de la tâche Update, dans les sections **Sources de mise à jour** et **Paramètres**, vous pouvez gérer les paramètres répertoriés dans le tableau ci-dessous.

Section Sources de mises à jour de la tâche Mise à jour

Paramètre	Description

Source des mises à jour	Le tableau contient la liste des sources de mises à jour des bases de données. Au cours de la mise à jour, l'application s'adresse aux sources de mise à jour dans l'ordre où celles-ci apparaissent dans le tableau.
	Ce tableau contient les colonnes suivantes :
	• **Adresse de la source** : adresse de la source de mises à jour.
	  • **Serveurs de mise à jour Kaspersky** qui hébergent les mises à jour des bases de données pour toutes les applications de Kaspersky (valeur par défaut).
	  • **Kaspersky Security Center** : Serveur d'administration de Kaspersky Security Center.
	  • Autres sources sur le réseau local ou sur Internet ajoutées par l'utilisateur : serveurs HTTP, HTTPS ou FTP ou répertoires sur les serveurs de réseau local.
	• **État** indique si la source de mises à jour est utilisée dans la tâche (**Utilisé** ou **Pas utilisé**). Vous pouvez modifier l'état en cochant ou en décochant la case **Utiliser cette source** dans la fenêtre **Source des mises à jour** qui s'ouvre lorsque vous cliquez sur le bouton **Modifier**.
	Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les sources de mise à jour dans le tableau.

Section Paramètres de la tâche Mise à jour

Paramètre	Description
Durée d'attente maximale de la réponse de la source des mises à jour (en secondes)	Temps d'attente maximal de la réponse à la demande de l'application en provenance de la source de mises à jour sélectionnée (en secondes). En l'absence de réponse à l'expiration de ce délai, l'événement relatif à la perte de connexion à la source de mises à jour est consigné dans le journal d'exécution des tâches. Valeurs admises : 0 à 120. Si vous saisissez la valeur 0, le délai d'attente de la réponse de la ressource choisie à la demande de l'application n'est pas limité. Valeur par défaut : 10 secondes.
Mode de téléchargement des mises à jour de l'application	Dans la liste déroulante, vous pouvez sélectionner le mode de téléchargement des mises à jour d'applications installées automatiquement (correctifs automatiques) : • **Ne pas télécharger**. Lorsque cette option est sélectionnée, les correctifs automatiques ne sont pas téléchargés automatiquement. • **Télécharger seulement**. Lorsque cette option est sélectionnée, les correctifs automatiques sont téléchargés automatiquement, mais ne sont pas installés sur les appareils clients (valeur par défaut). • **Télécharger et installer**. La sélection de cette option de la liste téléchargera et installera automatiquement les correctifs automatiques sur les appareils clients. Après avoir installé le correctif automatique, l'application redémarrera automatiquement.

Protection contre les menaces contre l'hôte

Protection contre les fichiers malicieux

Dans la Console d'administration, vous pouvez gérer la Protection contre les fichiers malicieux dans les propriétés de la stratégie (**Protection principale → Protection contre les fichiers malicieux**).

Paramètres du module Protection contre les fichiers malicieux

Paramètre	Description
Activer la Protection contre les fichiers malicieux	La case active ou désactive le module Protection contre les fichiers malicieux sur tous les appareils administrés. La case est cochée par défaut.
Mode de la Protection contre les fichiers malicieux	Cette liste déroulante permet de sélectionner le mode de fonctionnement du module Protection contre les fichiers malicieux : • **Mode intelligent** (valeur par défaut) analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture, s'il a été modifié. Si un processus accède plusieurs fois à un fichier au cours d'une certaine période et le modifie, l'application analyse à nouveau le fichier uniquement lorsque le processus le ferme pour la dernière fois. • **À l'accès** analyse le fichier lors de la tentative d'ouverture pour lecture, exécution ou modification. • **À l'accès et à la modification** analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture, s'il a été modifié.
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez **ajouter**, **modifier**, **supprimer**, **déplacer vers le haut** ou **déplacer vers le bas** les éléments dans le tableau.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez le bouton **Supprimer** pour exclure la zone sélectionnée de l'analyse.

Le bouton est accessible si au moins une zone d'analyse est sélectionnée dans le tableau.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère / dans le nom du fichier ou du répertoire. Par exemple, /dir/*/file ou /dir/*/*/file.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, /dir/**/file*/ ou /dir/file**/.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/file est un masque incorrect.

Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Où :

<id> est l'ID du conteneur.

<name> est le nom du conteneur

<path to local directory> est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : [container-id:<id>], [container-name:<name>], [image-id:<id>] et [image-name:<name>]/path to local directory>.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

Vous pouvez utiliser des masques (caractères ? et *) dans les noms et les identifiants.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la Protection contre les fichiers malicieux.

Paramètres de la Protection contre les menaces sur les fichiers

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si cette case est cochée, Kaspersky Endpoint Security analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en activant et en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les archives. La case est décochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si cette case est cochée, Kaspersky Endpoint Security analyse les archives autoextractibles. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est décochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, Kaspersky Endpoint Security analyse les fichiers des bases de messagerie. Si la case est décochée, Kaspersky Endpoint Security n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, Kaspersky Endpoint Security analyse les messages au format texte brut. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer les fichiers texte	Exclusion temporaire de l'analyse des fichiers au format texte. Si la case est cochée, Kaspersky Endpoint Security n'analysera pas les fichiers texte si ces fichiers ont été utilisés à nouveau par le même processus au cours des 10 minutes après la dernière analyse. Ce paramètre permet d'optimiser l'analyse des journaux de fonctionnement des applications. Si cette case est décochée, Kaspersky Endpoint Security analyse les fichiers texte. La case est décochée par défaut. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.
Ignorer les fichiers journaux de la base de données	Exclure temporairement les fichiers journaux de base de données de l'analyse. Si la case est cochée, l'application ne vérifiera pas le fichier journal de la base de données si le fichier journal est réutilisé par le même processus dans les 10 minutes suivant la dernière vérification. Ce paramètre permet d'optimiser la vérification des journaux de la base de données. Si la case à cocher est décochée, l'application vérifie les fichiers journaux de la base de données. La case est décochée par défaut. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.

Paramètre	Description
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, Kaspersky Endpoint Security interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 60.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, Kaspersky Endpoint Security analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *ObjectProcessed* pour tout objet analysé. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *ObjectProcessed*. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *ObjectNotProcessed*. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *ObjectNotProcessed*. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *PackedObjectDetected*. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *PackedObjectDetected*. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, Kaspersky Endpoint Security analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, Kaspersky Endpoint Security analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Paramètres de la Protection contre les menaces sur les fichiers

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; bloquer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application bloque l'accès à l'objet infecté. • **Bloquer**. Lorsque vous sélectionnez cette action, l'application bloque l'accès à l'objet infecté. Une fois désinfecté et supprimé, une copie de l'objet infecté sera placée dans la sauvegarde.

Exclusions de la Protection contre les fichiers malicieux

Une *exclusion de la protection* est un ensemble de conditions qui doivent être remplies pour que l'application Kaspersky Endpoint Security ne recherche pas de virus et autres applications malveillantes dans les objets. Vous pouvez également exclure des objets de l'analyse en fonction des masques et noms de menaces et configurer des exclusions pour les processus.

Dans la Console d'administration, vous pouvez configurer les exclusions de la Protection contre les fichiers malicieux dans les propriétés de la stratégie (**Protection principale** → **Exclusions de la Protection contre les fichiers malicieux**).

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Exclusions par processus	Ce groupe de paramètres contient le bouton **Configurer**, qui ouvre la fenêtre **Exclusions par processus**. Dans cette fenêtre, vous pouvez configurer l'exclusion de l'activité de processus de l'analyse.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions par processus

La fenêtre contient les zones d'exclusion en fonction des processus. La zone d'exclusion en fonction des processus vous permet de configurer l'exclusion de l'activité d'analyse du processus spécifié et des fichiers modifiés par le processus spécifié. Par défaut, la liste contient deux zones d'exclusion contenant les chemins d'accès aux Agents d'administration. Vous pouvez supprimer ces exclusions si nécessaire.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès complet au processus exclu.
État	L'état indique si cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Processus de confiance

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**. Le champ de saisie ne peut être vide.
Chemin d'accès au processus exclu	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse. Si un module de noyau mis à jour est utilisé pour intercepter les événements système, le processus spécifié est exclu de l'interception dans tous les espaces de noms.

Paramètre	Description
Appliquer aux processus enfants	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre **Chemin d'accès au processus exclu**. La case est décochée par défaut.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion de cette zone pour l'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.
Chemin d'accès aux fichiers modifiés	Le groupe de paramètres vous permet de définir des exclusions d'analyse pour les fichiers que le processus modifie. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si **Monté** ou **Partagé** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante des protocoles d'accès : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ de saisie ne peut être vide.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ **Chemin d'accès aux fichiers modifiés**. Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Analyse des logiciels malveillants

Dans la Console d'administration, vous pouvez rechercher les logiciels malveillants à l'aide de la tâche *Analyse des logiciels malveillants*.

Vous pouvez exécuter une tâche de groupe créée automatiquement, ainsi que créer et exécuter des tâches définies par l'utilisateur pour l'analyse. Vous pouvez gérer les paramètres d'analyse en modifiant les paramètres des tâches.

Dans les propriétés de la tâche *Recherche d'applications malveillantes*, dans la section **Paramètres**, vous pouvez gérer les paramètres répertoriés dans le tableau ci-dessous.

Paramètres d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse, des paramètres de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans les propriétés de la tâche *Recherche d'applications malveillantes*, dans la section **Exclusions**, vous pouvez personnaliser les zones d'exclusion, les exclusions par masque et par nom de menace.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez **ajouter**, **modifier**, **supprimer**, **déplacer vers le haut** ou **déplacer vers le bas** les éléments dans le tableau.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez le bouton **Supprimer** pour exclure la zone sélectionnée de l'analyse.

Le bouton est accessible si au moins une zone d'analyse est sélectionnée dans le tableau.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre <Nouvelle zone d'analyse>

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`

- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Paramètres de la zone d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse pendant le fonctionnement de la tâche Analyse des logiciels malveillants. L'application vous permet d'analyser les fichiers, les secteurs d'amorçage, la mémoire de l'appareil et les objets de démarrage automatique.

Paramètres de la zone d'analyse

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si la case est cochée, l'application analyse les fichiers. Si la case est décochée, l'application n'analyse pas les fichiers. La case est cochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si la case est cochée, l'application analyse les secteurs d'amorçage. Si cette case est décochée, l'application n'analyse pas les secteurs d'amorçage. La case est décochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, l'application ne vérifie pas les noyaux et les processus en cours d'exécution. La case est décochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si la case est cochée, l'application analyse les objets de démarrage. Si la case est décochée, l'application n'analyse pas les objets de démarrage. La case est décochée par défaut.
Appareils à analyser	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce bouton pour ouvrir la fenêtre **Zones d'analyse**, dans laquelle vous pouvez spécifier les appareils dont les secteurs de démarrage doivent être analysés.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètres d'analyse

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée de l'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans la section **Paramètres généraux de l'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. Cette case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.

Paramètre	Description
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est l'analyse la moins complète, avec une charge système minimale. • **Normal** est une analyse intermédiaire, avec une charge système équilibrée. • **Élevé** est l'analyse la plus complète, avec une charge système maximale. • **Recommandé** (par défaut) correspond au niveau optimal recommandé par les experts de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée. La case est décochée par défaut.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Une *exclusion de l'analyse* est un ensemble de conditions. Lorsque ces conditions sont réunies, Kaspersky Endpoint Security n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez également exclure des objets de l'analyse sur la base de masques et de noms de menaces.

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Analyse des zones critiques

Dans la Console d'administration, vous pouvez analyser les zones critiques du système d'exploitation de l'appareil protégé à l'aide de la tâche *Analyser les zones critiques*.

Vous pouvez créer et exécuter des tâches personnalisées d'analyse des zones critiques. Vous pouvez gérer les paramètres d'analyse en modifiant les paramètres des tâches.

Dans les propriétés de la tâche *Analyse des zones critiques*, dans la section **Paramètres**, vous pouvez gérer les paramètres répertoriés dans le tableau ci-dessous.

Paramètres de la tâche d'analyse des zones critiques

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse, des paramètres de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans les propriétés de la tâche *Analyse des zones critiques*, dans la section **Exclusions**, vous pouvez personnaliser les zones d'exclusion, les exclusions par masque et par nom de menace.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez **ajouter**, **modifier**, **supprimer**, **déplacer vers le haut** ou **déplacer vers le bas** les éléments dans le tableau.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez le bouton **Supprimer** pour exclure la zone sélectionnée de l'analyse.

Le bouton est accessible si au moins une zone d'analyse est sélectionnée dans le tableau.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`

- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Paramètres de la zone d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse pendant le fonctionnement de la tâche Analyse des zones critiques. Lors de l'exécution de la tâche, l'application analyse les fichiers, les secteurs d'amorçage, les objets de démarrage automatique, la mémoire des processus et la mémoire du noyau.

Paramètres de la zone d'analyse

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si cette case est cochée, Kaspersky Endpoint Security analyse les fichiers. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les fichiers. La case est décochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si cette case est cochée, Kaspersky Endpoint Security analyse les secteurs de démarrage. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les secteurs de démarrage. La case est cochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil. Si la case est cochée, Kaspersky Endpoint Security vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, Kaspersky Endpoint Security ne vérifie pas la mémoire du noyau ni les processus en cours d'exécution. La case est cochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si cette case est cochée, Kaspersky Endpoint Security analyse les objets de démarrage. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les objets de démarrage automatique. La case est cochée par défaut.
Appareils à analyser	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce bouton pour ouvrir la fenêtre **Zones d'analyse**, dans laquelle vous pouvez spécifier les appareils dont les secteurs de démarrage doivent être analysés.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètres d'analyse

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée de l'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans la section **Paramètres généraux de l'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. Cette case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.

Paramètre	Description
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est l'analyse la moins complète, avec une charge système minimale. • **Normal** est une analyse intermédiaire, avec une charge système équilibrée. • **Élevé** est l'analyse la plus complète, avec une charge système maximale. • **Recommandé** (par défaut) correspond au niveau optimal recommandé par les experts de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée. La case est décochée par défaut.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Une *exclusion de l'analyse* est un ensemble de conditions. Lorsque ces conditions sont réunies, Kaspersky Endpoint Security n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez également exclure des objets de l'analyse sur la base de masques et de noms de menaces.

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Surveillance des conteneurs

Dans la Console d'administration, vous pouvez configurer le module Surveillance des conteneurs dans les propriétés de la stratégie (**Paramètres généraux → Paramètres de l'Analyse du conteneur**).

Paramètres de surveillance des conteneurs

Paramètre	Description
Activer la surveillance des espaces de noms et des conteneurs	La case active ou désactive la vérification en temps réel des espaces des noms et des conteneurs. La case est cochée par défaut.
Action sur le conteneur en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur le conteneur en cas de détection d'un objet infecté lors de l'analyse : • L'option **Ignorer le conteneur** signifie que l'application n'effectue aucune action sur le conteneur lorsqu'un objet infecté est détecté. • L'option **Arrêter le conteneur** signifie que l'application arrête le conteneur suite à la détection d'un objet infecté. • **Arrêter en cas d'échec de la désinfection** (valeur par défaut) : l'application arrête le conteneur si la désinfection d'un objet infecté a échoué. Cette option est disponible lors de l'utilisation de l'application sous une licence qui active cette fonctionnalité.
Paramètres d'analyse de conteneur	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre Paramètres d'analyse des conteneurs.

Fenêtre Paramètres d'analyse de conteneur

Dans cette fenêtre, vous pouvez configurer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec le système d'administration des conteneurs Docker, de l'environnement CRI-O et des utilitaires Podman et runc.

Paramètres d'analyse de conteneur

Paramètre	Description
Utiliser Docker	Cette case active ou désactive l'utilisation du système d'administration des conteneurs Docker. La case est cochée par défaut.
Chemin du socket de Docker	Champ de saisie du chemin d'accès ou URI (ID universel de ressource) du socket de Docker. Valeur par défaut : /var/run/docker.sock.
Utiliser CRI-O	La case permet d'activer ou de désactiver l'utilisation de l'environnement CRI-O. La case est cochée par défaut.
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier de configuration CRI-O. Valeur par défaut : /etc/crio/crio.conf.
Utiliser Podman	La case permet d'activer ou de désactiver l'utilisation de l'utilitaire Podman. La case est cochée par défaut.
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier exécutable de l'utilitaire Podman. Valeur par défaut : /usr/bin/podman.
Dossier racine	Champ de saisie du chemin d'accès au dossier racine du stockage de conteneurs. Valeur par défaut : /var/lib/containers/storage
Utiliser runc	La case permet d'activer ou de désactiver l'utilisation de l'utilitaire runc. La case est cochée par défaut.

Paramètre	Description
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier exécutable de l'utilitaire runc. Valeur par défaut : /usr/bin/runc.
Dossier racine	Champ de saisie du chemin d'accès au dossier racine du stockage de l'état des conteneurs. Valeur par défaut : /run/runc.

Analyser les conteneurs

Dans la Console d'administration, vous pouvez analyser du conteneur et les images à l'aide de la tâche *Analyse du conteneur*.

Vous pouvez créer et exécuter des tâches personnalisées d'analyse du conteneur. Vous pouvez gérer les paramètres d'analyse en modifiant les paramètres des tâches.

Dans les propriétés de la tâche *Analyse du conteneur*, dans la section **Paramètres**, vous pouvez gérer les paramètres répertoriés dans le tableau ci-dessous.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration des paramètres d'analyse du conteneur et des paramètres généraux de l'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans les propriétés de la tâche *Analyse du conteneur*, dans la section **Exclusions**, vous pouvez également configurer des exclusions par masque et par nom de menace.

Fenêtre Paramètres d'analyse de conteneur

Cette fenêtre permet de configurer les paramètres d'analyse du conteneur et des images.

Paramètres d'analyse du conteneur et des images

Paramètre	Description
Analyser les conteneurs	La case active ou désactive l'analyse du conteneur. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les conteneurs à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les conteneurs à analyser. Par défaut, le masque * est utilisé (tous les conteneurs seront analysés).
Action en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur le conteneur en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer le conteneur** pour n'effectuer aucune action sur le conteneur lorsqu'un objet infecté a été détecté. • **Arrêter le conteneur** : arrête le conteneur à la suite de la détection d'un objet infecté. • **Arrêter en cas d'échec de la désinfection** (valeur par défaut) : arrêter le conteneur si l'objet infecté n'a pas pu être désinfecté ou si la menace n'a pas pu être éliminée. En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action **Arrêter le conteneur**.

Paramètre	Description
Analyser les images	La case active ou désactive l'analyse des images. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les images à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les images à analyser. Par défaut, le masque * est utilisé (toutes les images seront analysées).
Action en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur l'image en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer l'image** (valeur par défaut) : n'effectue aucune action sur l'image lorsqu'un objet infecté a été détecté. • **Supprimer l'image** lorsqu'un objet infecté a été détecté (déconseillé). Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.
Analyser chaque couche	Cette case active ou désactive l'analyse de toutes les couches des images et des conteneurs lancés. La case est décochée par défaut.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètres d'analyse

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée de l'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans la section **Paramètres généraux de l'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. Cette case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.

Paramètre	Description
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est l'analyse la moins complète, avec une charge système minimale. • **Normal** est une analyse intermédiaire, avec une charge système équilibrée. • **Élevé** est l'analyse la plus complète, avec une charge système maximale. • **Recommandé** (par défaut) correspond au niveau optimal recommandé par les experts de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Report du lancement des taches d'analyse si une analyse est déjà en cours. Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, supposons que l'application a lancé une tâche d'analyse complète selon la planification. Si un utilisateur tente de lancer une analyse rapide à partir de l'interface de l'application, Kaspersky Endpoint Security mettra en file d'attente cette tâche d'analyse rapide et la lancera automatiquement une fois que la tâche d'analyse complète sera terminée. La case est décochée par défaut.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Analyse des disques amovibles

Dans la Console d'administration, vous pouvez configurer les paramètres de l'analyse des disques amovibles dans les propriétés de la stratégie (**Tâches locales** → **Analyse des disques amovibles**).

Paramètres du module Analyse des disques amovibles

Paramètre	Description
Activer l'analyse des disques amovibles à la connexion à l'appareil	La case active ou désactive l'analyse des disques amovibles lors de la connexion à l'appareil de l'utilisateur. La case est décochée par défaut.
Action à réaliser en cas de connexion d'un disque amovible	La liste déroulante permet de sélectionner l'action que l'application va exécuter en cas de connexion de disques amovibles à l'appareil de l'utilisateur : • **Ne pas analyser** les disques amovibles lors de la connexion (valeur par défaut). • **Analyse rapide** : analyse uniquement les fichiers de certains types sur les disques amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray) et ne décompresse pas les objets composés. Une analyse rapide est effectuée avec les paramètres par défaut de la tâche *Analyse des zones critiques*. • **Analyse complète** : analyse tous les fichiers sur les disques amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray). Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Analyse des logiciels malveillants*.
Action à réaliser en cas de connexion d'un lecteur CD / DVD	La liste déroulante permet de sélectionner l'action que l'application va exécuter en cas de connexion de lecteurs CD/DVD et de disques Blu-ray à l'appareil de l'utilisateur : • **Ne pas analyser** les lecteurs CD/DVD et les disques Blu-ray à la connexion (valeur par défaut). • **Analyse rapide** : analyse uniquement les fichiers de certains types sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse rapide est effectuée avec les paramètres par défaut de la tâche *Analyse des zones critiques*. • **Analyse complète** : analyse tous les fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Analyse des logiciels malveillants*.
Bloquer l'accès au disque amovible pendant l'analyse	Cette case active ou désactive le blocage des fichiers à la connexion du disque lors de la tâche d'analyse. La case est décochée par défaut.

Articles utiles

Types de fichiers pour l'analyse rapide

Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx.

Détection comportementale

Dans la Console d'administration, vous pouvez gérer les paramètres de la Détection comportementale dans les propriétés de la stratégie (**Protection avancée** → **Détection comportementale**).

Paramètres du module Détection comportementale

Paramètre	Description
Activer la Détection comportementale	La case active ou désactive le module Détection comportementale. La case est cochée par défaut.
Action en cas de détection d'une activité malveillante	Action que Kaspersky Endpoint Security entreprendra lorsqu'elle détectera une activité malveillante dans le système d'exploitation : • **Bloquer** une application qui exécute une activité malveillante (par défaut). Kaspersky Endpoint Security termine le processus à l'origine de l'activité malveillante et enregistre dans le journal des événements les informations sur l'activité malveillante détectée. • **Informer** l'utilisateur. Kaspersky Endpoint Security ne termine pas le processus qui exécute une activité malveillante, consigne uniquement l'événement de détection d'une activité malveillante dans le journal des événements.
Utiliser les exclusions par processus	La case active ou désactive l'utilisation des exclusions par processus dans le fonctionnement du module Détection comportementale. La case est décochée par défaut. Cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Exclusions par processus**. Dans cette fenêtre, vous pouvez configurer l'exclusion de l'activité de processus de l'analyse.

Fenêtre Exclusions par processus

La fenêtre contient les zones d'exclusion en fonction des processus. La zone d'exclusion en fonction des processus vous permet de configurer l'exclusion de l'activité du processus spécifié de l'analyse.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès complet au processus exclu.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Processus de confiance

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**.
Chemin d'accès au processus exclu	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ de saisie ne peut être vide.

Paramètre	Description
Appliquer aux processus enfants	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre **Chemin d'accès au processus exclu**. La case est décochée par défaut.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion de cette zone pour l'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone pendant son fonctionnement. Si cette case est décochée, l'application inclut cette zone pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.
Exclure un processus de l'analyse par le module Détection comportementale	La case active ou désactive l'exclusion d'un processus de la vérification lorsque le module Détection comportementale est en cours d'exécution. La case est décochée par défaut.
Exclure le processus de la télémétrie MDR et EDR Expert (on-premises)	Cette case à cocher active ou désactive l'exclusion du processus de la télémétrie collectée par les modules MDR et EDR Expert (on-premises). La case est décochée par défaut.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Protection contre les Exploits

Dans la Console d'administration, vous pouvez configurer la Protection contre les Exploits dans les propriétés de la stratégie (**Protection avancée → Détection comportementale**).

Paramètres du module Protection contre les Exploits

Paramètre	Description
Activer la Protection contre les Exploits	Le case active ou désactive le module Protection contre les Exploits. La case est décochée par défaut.
Protection contre les Exploits	Le bouton **Configurer** ouvre la fenêtre **Exclusions de la Protection contre les Exploits**, dans laquelle vous pouvez configurer les exclusions d'analyse pour le module Protection contre les Exploits.
Action en cas de détection d'un Exploit	Action que l'application devra exécuter en cas de détection d'un Exploit : • **Bloquer** (valeur par défaut). L'application bloque les actions malveillantes de l'exploit et enregistre des informations à ce sujet dans le journal des événements. • **Informer**. L'application ne bloque pas les actions d'exploit, mais enregistre uniquement les informations sur la détection d'exploit dans le journal des événements.

Fenêtre Exclusions de la Protection contre les Exploits

Dans cette fenêtre, vous pouvez configurer les objets à exclure de l'analyse de la Protection contre les Exploits. L'application n'analysera pas les objets spécifiés. Par défaut, la liste des objets est vide.

Paramètres de l'exclusion de la Protection contre les Exploits

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
État	L'état indique si cette exclusion est appliquée par l'application.
Nom de la menace	Nom de la menace exclue de l'analyse.
Chemin d'accès au fichier ou au répertoire	Chemin d'accès complet au fichier ou répertoire exclu de l'analyse.
Somme de hachage du fichier	Somme de hachage du fichier exclu de l'analyse.
Commentaire	Commentaire relatif à l'exclusion d'analyse.

Par défaut, la tableau des exclusions est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Exclusion de la Protection contre les Exploits

Dans cette fenêtre, vous pouvez ajouter ou configurer une exclusion d'analyse par le module Protection contre les Exploits.

Paramètres de l'exclusion de la Protection contre les Exploits

Paramètre	Description
Utiliser le nom de la menace	La case active ou désactive l'utilisation d'une exclusion d'analyse d'un objet en fonction du nom de la menace détectée dans l'objet. La case est cochée par défaut.
Nom de la menace	Champ permettant de saisir le nom de la menace détectée dans l'objet. Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet. Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/. Ce champ est disponible si la case **Utiliser le nom de la menace** est cochée.
Utiliser la somme de hachage du fichier	Cette case active ou désactive l'utilisation des exclusions d'analyse de fichiers en fonction de leur valeur de hachage. La case est cochée par défaut.
Type de hachage de fichier	utilisez la liste déroulante pour sélectionner le type de hachage de fichier à utiliser pour exclure le fichier de l'analyse. • **MD5**. • **SHA256**. Cette liste déroulante est disponible si la case **Utiliser la somme de hachage du fichier** est cochée.
Somme de hachage du fichier	Ce champ vous permet de saisir la somme de hachage du fichier à utiliser pour exclure le fichier de l'analyse. Ce champ est disponible si la case **Utiliser la somme de hachage du fichier** est cochée.
Utiliser le chemin d'accès au fichier ou au répertoire	Cette case active ou désactive l'utilisation des exclusions d'analyse de fichiers en fonction du chemin d'accès au fichier dans lequel une menace a été détectée. La case est cochée par défaut.
Chemin d'accès au fichier ou au répertoire	Ce champ permet de saisir le chemin d'accès à un fichier ou un répertoire à exclure de l'analyse. Vous pouvez utiliser des symboles * et ? pour spécifier le chemin. Il est disponible si la case **Utiliser le chemin d'accès au fichier ou au répertoire** est cochée.

Paramètre	Description
Commentaire	Champ de saisie pour un commentaire (facultatif).
Utiliser cette exclusion	La case à cocher active ou désactive l'utilisation de cette exclusion pendant l'exécution de l'application. La case est cochée par défaut.

Protection contre le chiffrement

Dans la Console d'administration, vous pouvez gérer les paramètres de Protection contre le chiffrement dans les propriétés de la stratégie (**Protection avancée → Protection contre le chiffrement**).

Paramètres du module Protection contre le chiffrement

Paramètre	Description
Activer la protection contre le chiffrement	La case active ou désactive la protection des fichiers des répertoires locaux avec accès réseau par protocoles SMB/NFS contre le chiffrement à distance malveillant. La case est décochée par défaut.
Zones de protection	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse et des paramètres de la protection.
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez **ajouter**, **modifier**, **supprimer**, **déplacer vers le haut** ou **déplacer vers le bas** les éléments dans le tableau.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez le bouton **Supprimer** pour exclure la zone sélectionnée de l'analyse.

Le bouton est accessible si au moins une zone d'analyse est sélectionnée dans le tableau.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Dans cette fenêtre, vous pouvez ajouter ou configurer la zone de protection du module Protection contre le chiffrement.

Paramètres de la zone de protection

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone de protection. Ce nom sera affiché dans le tableau de la fenêtre Zones d'analyse. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone de protection pendant le fonctionnement du module. Si cette case est décochée, l'application ne traite pas cette zone de protection pendant le fonctionnement du module. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement du module en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** : répertoires locaux. • **Partagé** affiche les ressources du système de fichiers du serveur accessibles via le protocole Samba ou NFS. • **Tous les éléments partagés** (valeur par défaut) : affiche les ressources du système de fichiers du serveur accessibles via les protocoles Samba et NFS.
	Si **Partagé** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone de protection. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ ne peut être vide.
Masques	La liste contient les masques des noms des objets analysés par l'application pendant le fonctionnement du module Protection contre le chiffrement. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère * (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Fenêtre Paramètres de la protection

Paramètres de la protection

Paramètre	Description
Action en cas de détection d'un chiffrement	Action que Kaspersky Endpoint Security effectuera lorsqu'un chiffrement malveillant est détecté : • **Informer** l'utilisateur. Kaspersky Endpoint Security ne bloque pas l'appareil effectuant le chiffrement ; il enregistre uniquement l'événement de détection d'un chiffrement malveillant dans le journal des événements. • **Bloquer** l'appareil effectuant le chiffrement (par défaut).
Bloquer un appareil douteux pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un appareil douteux (en minutes). À l'expiration du délai indiqué, l'application Kaspersky Endpoint Security retire les hôtes douteux de la liste des appareils bloqués. L'accès de l'hôte aux ressources de fichier réseau est automatiquement restauré une fois qu'il a été supprimé de la liste d'hôtes douteux. Si un hôte compromis est bloqué et si vous modifiez cette valeur de paramètre, la durée de blocage de cet hôte ne change pas. La durée de blocage n'est pas une valeur dynamique et se calcule au moment du blocage. Valeurs disponibles : entier de 1 à 2147483647. Valeur par défaut : 30.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

- Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** pour les répertoires locaux. • **Monté** pour les répertoires montés. • **Tous les systèmes montés distants** pour tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** pour les répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** pour les répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** pour les ressources du système de fichiers de l'appareil indiquées dans le champ ci-dessous.
	Si **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez saisir dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des masques et des tags pour spécifier le chemin. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers et si l'élément **Personnalisé** est sélectionné dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Comment utiliser les tags

Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image :

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Où :

`<id>` est l'ID du conteneur.

`<name>` est le nom du conteneur

`<path to local directory>` est le chemin d'accès au répertoire local.

Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`.

Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance.

Par exemple :

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Kaspersky Security Network

Dans la Console d'administration, vous pouvez configurer l'utilisation de Kaspersky Security Network dans Kaspersky Endpoint Security dans les propriétés de la stratégie (**Protection avancée → Kaspersky Security Network**).

Le contenu de la Déclaration de Kaspersky Security Network est disponible dans la fenêtre **Déclaration de Kaspersky Security Network** qui s'ouvre via le lien **Déclaration de Kaspersky Security Network**.

Les informations sur la disponibilité du KSN sont affichées dans Kaspersky Security Center en utilisant l'état de l'appareil client (*OK, Critique, Avertissement*) dans la liste des appareils administrés sous l'onglet **Appareils**.

Paramètres de Kaspersky Security Network

Paramètre	Description
Déclaration de Kaspersky Security Network	Cliquez sur ce lien pour ouvrir la fenêtre **Déclaration de Kaspersky Security Network**. Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Security Network.
Kaspersky Security Network (KSN)	Le groupe affiche des informations sur le mode d'utilisation de KSN ou sur le fait que KSN n'est pas utilisé dans le fonctionnement de Kaspersky Endpoint Security. En cliquant sur le bouton **Modifier**, une fenêtre s'ouvre dans laquelle vous pouvez configurer l'utilisation de Kaspersky Security Network.
Activer le mode cloud	En *mode Cloud*, Kaspersky Endpoint Security utilise une version allégée des bases antivirus, ce qui réduit de moitié environ la charge sur la RAM de l'ordinateur. La case est disponible si KSN est activé. La case est cochée si, lors de la création de la stratégie, vous avez accepté les termes de la Déclaration de Kaspersky Security Network et utilisé le mode avancé de KSN. Le mode est activé ou désactivé après la prochaine mise à jour de la base de données de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Utiliser le Serveur d'administration comme serveur proxy KSN	Si la case est sélectionnée, l'application Kaspersky Endpoint Security interagit avec les serveurs KSN à l'aide du service du serveur proxy KSN sur le Serveur d'administration. La case est cochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. En mode Light Agent, l'application ne peut communiquer avec l'infrastructure KSN que via un serveur proxy KSN.
Utiliser les serveurs KSN si le proxy KSN n'est pas disponible	Si la case est sélectionnée, l'application Kaspersky Endpoint Security communique directement avec les serveurs KSN lorsque le service proxy KSN n'est pas disponible. La case est cochée par défaut. La case est disponible si la case **Utiliser le Serveur d'administration comme serveur proxy KSN** est sélectionnée. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.

Paramètres de Kaspersky Security Network

Cette fenêtre permet de configurer les paramètres de participation à Kaspersky Security Network.

Paramètres de Kaspersky Security Network

Paramètre	Description
En savoir plus	Cliquez sur ce lien pour accéder au site Internet de Kaspersky.
Ne pas utiliser Kaspersky Security Network	En sélectionnant cette option, vous refusez d'utiliser Kaspersky Security Network.
Mode KSN de base	En sélectionnant cette option, vous acceptez les conditions d'utilisation de Kaspersky Security Network. Vous pourrez recevoir des informations de la base de connaissances en ligne de Kaspersky sur la réputation des fichiers, des ressources Web et des logiciels.
Mode étendu de KSN	En sélectionnant cette option, vous acceptez les conditions d'utilisation de Kaspersky Security Network. Vous pourrez recevoir des informations de la base de connaissances en ligne de Kaspersky sur la réputation des fichiers, des ressources Web et des logiciels. En outre, des statistiques et informations anonymes sur les types et sources de différentes menaces seront envoyées pour améliorer Kaspersky Security Network dans Kaspersky.
Déclaration de Kaspersky Security Network	Le lien ouvre la fenêtre **Déclaration de Kaspersky Security Network** dans laquelle vous pouvez lire le texte de la Déclaration de Kaspersky Security Network.

Déclaration de Kaspersky Security Network

Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Security Network et d'en accepter les dispositions.

Paramètres de Kaspersky Security Network

Paramètre	Description
Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network	En sélectionnant cette option, vous confirmez que vous souhaitez utiliser Kaspersky Security Network et que vous avez entièrement lu, compris et accepté les dispositions de la déclaration de Kaspersky Security Network affichée. L'option est disponible si vous avez sélectionné l'option **Mode KSN de base** ou **Mode étendu de KSN** dans la fenêtre **Paramètres de Kaspersky Security Network**.
Je n'accepte pas les conditions de la Déclaration de Kaspersky Security Network	En choisissant cette option, vous confirmez que vous ne souhaitez pas utiliser Kaspersky Security Network L'option est disponible si vous avez sélectionné l'option **Mode KSN de base** ou **Mode étendu de KSN** dans la fenêtre **Paramètres de Kaspersky Security Network**.

Déclaration de Kaspersky Private Security Network

Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Private Security Network et d'en accepter les dispositions.

Paramètres de Kaspersky Security Network

Paramètre	Description
Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network	En sélectionnant cette option, vous confirmez que vous souhaitez participer au Kaspersky Security Network et que vous avez entièrement lu, compris et accepté les dispositions de la déclaration de Kaspersky Private Security Network affichée.
Je n'accepte pas les conditions de la Déclaration de Kaspersky Security Network	En choisissant cette option, vous confirmez que vous ne souhaitez pas utiliser Kaspersky Security Network

Protection BadUSB

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (**Protection principale → Protection BadUSB**).

Paramètres du module Protection BadUSB

Paramètre	Description
Activer la protection BadUSB	La case active ou désactive le module Protection BadUSB. Le module est désactivé par défaut.
Nombre maximal de tentatives d'autorisation de l'appareil USB	Bloque automatiquement un appareil USB si le code d'autorisation est saisi incorrectement un nombre de fois spécifié. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affichera la durée de verrouillage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.
Verrouillage de l'appareil lorsque le nombre maximal de tentatives d'autorisations est atteint (min.)	La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs autorisées vont de 1 à 180 minutes.
Interdire l'utilisation du clavier virtuel pour autoriser les appareils USB	Si le commutateur est activé, l'application bloque l'utilisation du clavier virtuel pour autoriser l'appareil USB à partir duquel la saisie du code d'autorisation est impossible.
Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB	Si ce bouton bascule est activé, l'application interdit l'utilisation d'un code-barres pour l'autorisation d'un appareil USB à partir duquel la saisie du code d'autorisation est impossible.

Protection des connexions réseau et des moyens de communications

Protection contre les menaces par emails

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (**Protection principale → Protection contre les menaces par emails**).

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Protection contre les menaces par emails	La case active ou désactive le module Protection contre les menaces par emails. Le module est activé par défaut.
Configurer (Paramètres de la protection)	Cliquer sur le bouton ouvre la fenêtre **Paramètres de la Protection contre les menaces par emails**, où vous pouvez configurer la zone de protection contre les menaces par emails et les paramètres d'analyse des fichiers composés.
Configurer (Filtre de pièces jointes)	Cliquer sur le bouton ouvre la fenêtre **Filtre de pièces jointes**, où vous pouvez configurer le filtrage des pièces jointes de vos emails.
Utiliser l'analyse heuristique **Niveau de l'analyse heuristique**	La case active ou désactive l'utilisation de l'analyseur heuristique. Lors de l'analyse des fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions exécutées dépend du niveau d'analyseur heuristique sélectionné. Celui-ci définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse heuristique. Par défaut, l'analyse heuristique est activée avec le niveau moyen.

Paramètre	Description
Actions en cas de détection d'une menace	Action effectuée par la Protection contre les menaces par emails lorsqu'une menace est détectée dans un email : • **Désinfecter ; supprimer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. Cette action est sélectionnée par défaut. • **Désinfecter ; bloquer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. • **Bloquer**. Si un objet infecté est détecté dans un message entrant, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. Ce paramètre ne s'applique pas aux messages sortants. Si un objet infecté est détecté dans un message sortant, l'application bloque son envoi.

Fenêtre Paramètres de la protection contre les menaces par emails

Cette fenêtre permet de configurer la zone de protection contre les menaces par emails et les paramètres d'analyse des fichiers composés.

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Zone de protection	*Zone de protection* : les objets que le module vérifie pendant son fonctionnement : messages entrants et sortants ou uniquement messages entrants. Par défaut, l'option **Messages entrants et sortants** est sélectionnée.
Analyser les archives jointes	Active et désactive la vérification des archives jointes. Analyse des archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). La case est cochée par défaut.
Analyser les fichiers joints des applications Office	Active ou désactive la vérification des fichiers joints aux formats Office. L'application analyse les fichiers au format Office de moins de 1 Mo, quel que soit l'état de la case. La case est cochée par défaut.
Ne pas analyser les archives de plus de (Mo)	Si la case est cochée, le module Protection contre les menaces par emails exclut de l'analyse les archives jointes aux messages électroniques dont la taille dépasse celle spécifiée. Si cette case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques. La case est décochée par défaut.
Limiter le temps d'analyse des archives à (sec.)	Si la case est cochée, la durée d'analyse des archives jointes aux messages est limitée à la période spécifiée. La case est décochée par défaut.

Fenêtre Filtre des pièces jointes

Dans cette fenêtre, vous pouvez configurer le filtrage des pièces jointes aux emails.

Paramètres de filtrage des pièces jointes

Paramètre	Description
Ne pas appliquer le filtre	Si cette option est sélectionnée, la Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques.
Renommer les pièces jointes de types spécifiés	Lorsque cette option est sélectionnée, la Protection contre les menaces par emails remplace le dernier caractère de l'extension des fichiers joints des types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir. Sélectionné par défaut.
Supprimer les pièces jointes des types spécifiés	Lorsque cette option est sélectionnée, la Protection contre les menaces par emails supprime les pièces jointes des types de fichiers spécifiés des messages électroniques. Vous pouvez spécifier les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Tableau des types de pièces jointes	Le tableau indique les types de pièces jointes qui doivent être renommées ou supprimées des messages électroniques. Vous pouvez ajouter, modifier et supprimer des types de pièces jointes à l'aide des boutons du même nom.

Protection contre les menaces Internet

Dans la Console d'administration, vous pouvez configurer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (**Protection principale → Protection contre les menaces Internet**).

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Activer la Protection contre les menaces Internet	Cette case active ou désactive le module Protection contre les menaces Internet. La case est décochée par défaut.
Adresses Internet de confiance	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Adresses Internet de confiance** dans laquelle vous pouvez établir une liste d'adresses Internet de confiance. L'application n'analyse pas le contenu des sites Internet dont l'adresse figure dans cette liste.
Action en cas de détection d'une menace	Action que l'application effectue sur les ressources Internet où un objet dangereux a été détecté : • **Bloquer** l'accès à tout objet dangereux détecté dans le trafic Internet, affiche une notification concernant la tentative d'accès bloqué et enregistre les informations sur l'objet dangereux dans le journal (valeur par défaut). • **Informer** l'utilisateur lorsqu'un objet dangereux est détecté dans le trafic Internet. La Protection contre les menaces Internet autorise le téléchargement de cet objet sur l'appareil. Dans ce cas, l'application consigne des informations sur l'objet dangereux et ajoute des informations relatives à ce dernier dans la liste des menaces actives.
Paramètres d'analyse	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Paramètres d'analyse** dans laquelle vous pouvez configurer les paramètres d'analyse du trafic entrant.

Fenêtre Adresses Internet de confiance

Cette fenêtre permet d'ajouter des adresses et des pages Internet au contenu desquelles vous faites confiance.

Vous pouvez ajouter uniquement des adresses Internet de confiance HTTP/HTTPS à cette liste. Vous pouvez utiliser des masques pour spécifier des adresses Internet. L'utilisation de masques dans le but de définir des adresses IP n'est pas prise en charge. Par défaut, la liste est vide. Vous pouvez ajouter, modifier et supprimer des adresses Internet dans la liste.

Comment spécifier des masques

Lors de la création d'un masque d'adresse, vous pouvez saisir l'astérisque (*) comme caractère générique pour un ou plusieurs caractères. Si vous saisissez ainsi le masque d'adresse *abc*, il sera appliqué à toutes les ressources Internet contenant la séquence abc (par exemple, www.virus.com/download_virus/page_0-9abcdef.html). Pour inclure l'astérisque dans le masque d'adresse en tant que caractère et non en tant que masque, saisissez deux fois le caractère * (par exemple, www.virus.com/**/page_0-9abcdef.html signifie www.virus.com/*/page_0-9abcdef.html).

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse du trafic entrant pendant le fonctionnement du module Protection contre les menaces Internet.

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Détecter les objets malveillants	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet malveillantes. La case est cochée par défaut.
Détecter les liens de phishing	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet de phishing. La case est cochée par défaut.
Détecter les liens de phishing à l'aide de l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique pour la détection des liens de phishing. Cette case est disponible si la case **Détecter les liens de phishing** est cochée et elle est sélectionnée par défaut.
Détecter les applications publicitaires	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet d'applications publicitaires. La case est décochée par défaut.
Détecter les applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données	Cette case active ou désactive la vérification des liens par rapport aux bases de données des applications légitimes qui pourraient être détournées par des individus malintentionnés pour nuire aux appareils ou aux données. La case est décochée par défaut.

Protection contre les menaces réseau

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces réseau dans les propriétés de la stratégie (**Protection principale → Protection contre les menaces réseau**).

Paramètres du module Protection contre les menaces réseau

Paramètre	Description
Activer la Protection contre les menaces réseau	La case active ou désactive la Protection contre les menaces réseau. La case est décochée par défaut.
Action en cas de détection d'une menace	Actions à entreprendre en cas de détection d'une activité réseau caractéristique des attaques réseau : • **Informer** l'utilisateur. L'application autorise l'activité réseau, consigne dans le journal les informations sur l'activité réseau détectée. • **Bloquer** l'activité réseau de l'appareil attaquant et consigner les informations sur l'activité réseau détectée (valeur par défaut) dans le journal.
Bloquer les hôtes attaquants	La case active ou désactive le blocage de l'activité réseau en cas de détection d'une tentative d'attaque réseau. La case est cochée par défaut.

Paramètre	Description
Bloquer l'hôte attaquant pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un appareil attaquant (en minutes). Une fois le délai spécifié écoulé, l'application Kaspersky Endpoint Security autorise l'activité réseau en provenance de cet appareil. Valeurs disponibles : entier de 1 à 32768. Valeur par défaut : 60.
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**, qui ouvre la fenêtre **Exclusions**, dans laquelle vous pouvez spécifier une liste d'adresses IP. Les attaques réseau provenant de ces adresses IP ne seront pas bloquées.

Fenêtre Exclusions

Cette fenêtre permet d'ajouter les adresses IP qui ne seront pas bloquées en cas d'attaques réseau.

Par défaut, la liste est vide.

Vous pouvez ajouter, modifier et supprimer des adresses IP dans la liste. Vous pouvez spécifier des adresses IP aux formats IPv4 et IPv6.

Gestion du pare-feu

Dans la Console d'administration, vous pouvez configurer les paramètres de gestion du pare-feu dans les propriétés de la stratégie (**Protection principale → Gestion du pare-feu**).

Paramètres du module Gestion du pare-feu

Paramètre	Description
Activer la tâche de gestion du pare-feu	La case active ou désactive le module Gestion du pare-feu. La case est décochée par défaut.
Règles de paquet réseau	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Règles pour les paquets réseau**. Cette fenêtre permet de configurer les règles de paquets réseau exécutées par le module Gestion du pare-feu lorsqu'il détecte la tentative de connexion réseau.
Réseaux disponibles	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Réseaux disponibles**. Cette fenêtre permet de configurer une liste de réseaux que le module Gestion du pare-feu va surveiller.
Connexions entrantes	Cette liste déroulante permet de sélectionner une action à réaliser sur les connexions réseau entrantes : • **Autoriser** les connexions réseau (valeur par défaut). • **Bloquer** les connexions réseau entrantes.
Paquets entrants	Dans cette liste déroulante, vous pouvez sélectionner une action à effectuer pour les paquets entrants : • **Autoriser** les paquets entrants (valeur par défaut). • **Bloquer** les paquets entrants.
Toujours ajouter les règles d'autorisation pour les ports de l'Agent d'administration	Cette case active ou désactive l'ajout automatique de règles d'autorisation pour les ports de l'Agent d'administration. La case est cochée par défaut.

Fenêtre Règles de paquet réseau

Le tableau **Règles de paquet réseau** contient des règles de paquet réseau que le module Gestion du pare-feu utilisera pour surveiller l'activité réseau. Pour les règles de paquet réseau, vous pouvez configurer les paramètres décrits dans le tableau ci-dessous.

Paramètres des règles de paquet de réseau

Paramètre	Description
Nom	Le nom de la règle de paquet réseau.
Action	Action que le module Gestion du pare-feu doit effectuer suite à la détection de l'activité réseau.
Adresse locale	Adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
Adresse à distance	Adresses réseau des appareils à distance qui peuvent envoyer et/ou recevoir des paquets réseau.
Enregistrement des événements dans le journal	Cette colonne indique si l'application enregistrera ou non les actions de règles de paquets réseau dans le rapport. Si la colonne indique **Oui**, l'application enregistre les actions de la règle de paquet réseau dans le journal. Si la colonne indique **Non**, l'application n'enregistre pas les actions de la règle de paquet réseau.

Par défaut, le tableau des règles de paquet réseau est vide.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les règles de paquet réseau dans le tableau.

Fenêtre Ajout d'une règle de paquet réseau

Cette fenêtre permet de configurer les paramètres de la règles de paquet réseau ajouté.

Paramètres des règles pour les paquets réseau

Paramètre	Description
Protocole.	Vous pouvez sélectionner le type de protocole de transfert de données pour lequel vous souhaitez surveiller l'activité réseau : • **Tous** (valeur par défaut) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Direction	Vous pouvez définir la direction de l'activité réseau surveillée : • **Paquets entrants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les paquets entrants. • **Entrant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les connexions entrantes. • **Entrants/Sortants** (valeur par défaut). Si cet élément est sélectionné, le module Gestion du pare-feu contrôle à la fois les connexions entrantes et sortantes. • **Paquets entrants/sortants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle à la fois les paquets entrants et sortants. • **Paquets sortants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les paquets sortants. • **Sortant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les connexions sortantes.
Type ICMP	Vous pouvez indiquer le type ICMP. Le module Gestion du pare-feu contrôle les messages d'un type spécifié envoyés par un hôte ou une passerelle. Si vous avez choisi l'option **Spécifié**, le champ de saisie du type ICMP s'affiche. Cette fenêtre s'affiche uniquement si vous avez sélectionné les protocoles de transfert de données **ICMP** ou **ICMPv6** dans la liste déroulante **Protocole**.
Code ICMP	Vous pouvez préciser le code ICMP. Le module Gestion du pare-feu surveillera les messages du type spécifié dans le champ **Type ICMP** et avec le code spécifié dans le champ **Code ICMP**, envoyés par l'hôte ou la passerelle. Si vous avez choisi l'option **Spécifié**, le champ de saisie du code ICMP s'affiche. Cette fenêtre s'affiche uniquement si vous avez sélectionné les protocoles de transfert de données **ICMP** ou **ICMPv6** dans la liste déroulante **Protocole**.

Paramètre	Description
Ports distants	Vous pouvez spécifier le numéro de port ou la plage de numéros de ports des appareils à distance entre lesquels la connexion doit être contrôlée. Si vous avez choisi l'option **Spécifié**, le champ de saisie des numéros des ports s'affiche. Cette fenêtre s'ouvre uniquement si vous avez sélectionné les protocoles de transfert de données **TCP** ou **UDP** dans la liste déroulante **Protocole**.
Ports locaux	Vous pouvez spécifier le numéro de port ou la plage de numéros de ports des appareils locaux entre lesquels la connexion doit être contrôlée. Si vous avez choisi l'option **Spécifié**, le champ de saisie des numéros des ports s'affiche. Cette fenêtre s'ouvre uniquement si vous avez sélectionné les protocoles de transfert de données **TCP** ou **UDP** dans la liste déroulante **Protocole**.
Adresses à distance	Vous pouvez préciser les adresses réseau des appareils distants qui peuvent envoyer et recevoir des paquets réseau. • **Toute adresse** (valeur par défaut). Si cette option est sélectionnée, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils distants avec toute adresse IP. • **Adresse ou plage d'adresses spécifiée**. Si vous sélectionnez cette option, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils à distance portant les adresses IP spécifiées dans le champ en-dessous. En cliquant sur le bouton **Ajouter** au-dessus du tableau, vous ouvrez la fenêtre **Ajout d'adresses IP**, dans laquelle vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil. • **Par type de réseau**. Si vous avez sélectionné cette option, la règle du réseau contrôle les paquets réseau envoyés et reçus par des appareils distants avec des adresses IP associées au type de réseaux sélectionné dans la liste déroulante : **Réseaux publics**, **Réseaux locaux** ou **Réseaux approuvés**.
Adresses locales	Vous pouvez renseigner les adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et recevoir des paquets réseau. • **Toute adresse** (valeur par défaut). Si cette option est sélectionnée, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils hébergeant Kaspersky Endpoint Security et portant n'importe quelle adresse IP. • **Adresse ou plage d'adresses spécifiée**. Si cette option est sélectionnée, la règle réseau contrôle les adresses réseau des appareils sur lesquels Kaspersky Endpoint Security est installé et qui peuvent envoyer et recevoir des paquets réseau. Ces adresses réseau sont spécifiées dans le tableau ci-dessous. En cliquant sur le bouton **Ajouter** au-dessus du tableau, vous ouvrez la fenêtre **Ajout d'adresses IP**, dans laquelle vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil.
Action	Vous pouvez définir l'action que le module Gestion du pare-feu effectuera en cas de détection de l'activité réseau : • **Bloquer** l' activité réseau. • **Autoriser** l'activité réseau (valeur par défaut).
Enregistrement des événements dans le journal	Vous pouvez indiquer si les actions de la règle de réseau doivent être prises en compte dans le rapport.
Nom de la règle	Le champ de saisie pour le nom de la règle de paquet réseau.

Fenêtre Ajout d'adresses IP

Dans cette fenêtre, vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil.

Vous pouvez spécifier plusieurs adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie.

Fenêtre Réseaux disponibles

Le tableau **Réseaux disponibles** contient les réseaux que le module Gestion du pare-feu va surveiller. Par défaut, le tableau des réseaux disponibles est vide.

Paramètres Réseaux disponibles

Paramètre	Description
Adresse IP ;	Adresse IP du réseau.
Type de réseau	Les types de réseau (**Réseau public**, **Réseau local** ou **Réseau de confiance**).

Vous pouvez ajouter, modifier et supprimer les réseaux disponibles.

Fenêtre Connexion réseau

Cette fenêtre permet de configurer la connexion réseau que le module Gestion du pare-feu surveillera.

Connexion réseau

Paramètre	Description
Adresse IP ;	Champ de saisie de l'adresse IP du réseau.
Type de réseau	Vous pouvez sélectionner le type de réseau : • **Réseau public**. • **Réseau local**. • **Réseau de confiance**.

Contrôles de sécurité

Contrôle des appareils

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle des appareils dans les propriétés de la stratégie (**Contrôles de sécurité → Contrôle des appareils**).

Paramètres du contrôle des appareils

Paramètre	Description
Activer le contrôle des appareils	Cette case active ou désactive le module Contrôle des appareils. La case est cochée par défaut.
Appareils de confiance	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce lien pour ouvrir la fenêtre **Appareils de confiance**. Dans cette fenêtre, vous pouvez ajouter un appareil à la liste des appareils de confiance.
Mode de fonctionnement du Contrôle des appareils	Mode de fonctionnement de l'application lors de la tentative d'accès à un appareil dont l'accès est interdit conformément aux paramètres du Contrôle des appareils : • **Informer**. Si vous sélectionnez cette option, Kaspersky Endpoint Security teste le mode d'accès sélectionné et génère un événement relatif à la tentative détectée d'accès à un appareil. • **Bloquer** (valeur par défaut). Si vous sélectionnez cette option, Kaspersky Endpoint Security applique le mode d'accès défini pour l'appareil ou le bus.
Paramètres du Contrôle des appareils	Le groupe de paramètres contient les boutons qui, lorsqu'ils sont cliqués, ouvrent des fenêtres dans lesquelles vous pouvez configurer le mode d'accès aux appareils en fonction de leur type et le mode d'accès aux bus de connexion.
Autoriser les demandes d'accès temporaire	Si cette case est cochée, l'utilisateur peut demander un accès temporaire à l'appareil bloqué dans l'interface graphique de l'application ou en ligne de commande.
Modèles de messages	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Modèles de messages**.

Fenêtre Appareils de confiance

Le tableau contient la liste des appareils de confiance. Par défaut, le tableau est vide.

Paramètres de l'appareil de confiance.

Paramètre	Description
ID de l'appareil	ID d'un appareil de confiance.
Nom de l'appareil	Nom d'un appareil de confiance.
Type d'appareil.	Type d'un appareil de confiance (par exemple, Disque dur ou Lecteur de carte intelligente).
Nom d'hôte	Nom de l'appareil client auquel se connecte un appareil de confiance.
Utilisateur ou groupe	Le nom d'utilisateur ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé.
Commentaire	Commentaire lié à un appareil de confiance.

Vous pouvez ajouter des appareils à la liste des appareils de confiance à l'aide du bouton **Ajouter** en procédant comme suit :

- Spécifier l'identifiant de l'appareil ou le masque de l'identifiant (**Ajouter → Ajouter un appareil par identifiant ou masque**).
- Sélectionner l'appareil souhaité dans la liste des appareils détectés sur les appareils administrés (**Ajouter → Sélectionner l'appareil dans la liste des appareils détectés sur les appareils clients**).
- Sélectionner l'appareil nécessaire dans la liste des appareils détectés dans les événements du Contrôle des appareils de Kaspersky Security Center (**Ajouter → Ajouter un appareil en fonction des événements**).

Vous pouvez modifier et supprimer des appareils de confiance dans le tableau.

Vous pouvez également exporter la liste des appareils ajoutés dans un fichier en cliquant sur le bouton **Avancés → Exporter les éléments sélectionnés** ou sur le bouton **Avancés → Exporter tout** et importer une liste d'appareils à partir d'un fichier JSON à l'aide du bouton **Avancés → Importer**.

Trois modes d'importation sont disponibles :

- **Fusionner avec ceux qui existent** : fusionne les listes d'appareils de confiance lors de l'importation. Si le fichier contient déjà un enregistrement pour un appareil avec le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figuraient pas auparavant dans la liste.
- **Ajouter à ceux qui existent** : compléter la liste des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.
- **Remplacer ceux qui existent** : remplacer la liste des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste du fichier.

Fenêtre Appareil de confiance (ID de l'appareil)

Cette fenêtre permet d'ajouter un appareil à la liste des appareils de confiance sur la base de son ID.

Ajout d'un appareil par ID

Paramètre	Description
ID de l'appareil	Champ de saisie d'ID ou de masque d'ID de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance. Pour indiquer un identifiant, vous pouvez utiliser des masques * (toute séquence de caractères) ou ? (n'importe quel caractère). Par exemple, vous pouvez indiquer un masque USBSTOR* pour autoriser l'accès à toutes les clés USB.
Recherche sur les appareils	Un clic sur le bouton affiche les appareils trouvés par l'identifiant ou le masque spécifié sur les appareils clients connectés. Le bouton est disponible quand le champ **ID de l'appareil** contient une valeur.

Paramètre	Description
Appareils trouvés	Ce tableau contient les colonnes suivantes : • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **ID de l'appareil** : identifiant de l'appareil trouvé. • **Nom de l'appareil** : nom de l'appareil trouvé. • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé.
Commentaire	Champ de saisie de commentaires au sujet de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance (facultatif).
Autoriser l'accès aux utilisateurs et/ou aux groupes d'utilisateurs	Un champ qui affiche le nom de l'utilisateur et/ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé. La valeur par défaut est **\Everyone** (tous les utilisateurs).
Configurer	Cliquer sur le bouton ouvre la fenêtre Accès à un appareil de confiance.

Fenêtre Appareils sur les appareils clients

Dans cette fenêtre, vous pouvez ajouter un appareil à une liste d'appareils de confiance en sélectionnant dans une liste d'appareils découverts sur les appareils clients administrés.

Les informations sur les appareils existants sont disponibles uniquement si une stratégie active est créée et s'il y a eu une synchronisation avec l'Agent d'administration (fonctionne dans les limites spécifiées dans la stratégie de l'Agent d'administration, 15 minutes par défaut).

Lorsque vous créez une stratégie inactive, la liste sera vide.

Ajout d'appareils à partir de la liste des appareils détectés sur les appareils clients administrés

Paramètre	Description
Nom d'hôte	Champ de saisie du nom ou du masque du nom de l'appareil administré pour lequel vous souhaitez trouver les appareils connectés. Le masque par défaut est *, qui représente tous les appareils administrés.
Type d'appareil.	Cette liste déroulante permet de définir le type d'appareil connecté à rechercher (par exemple, Disques durs ou Lecteurs de carte intelligente). L'option sélectionnée par défaut est **Tous les appareils**.
ID de l'appareil	Champ de saisie de l'ID ou du masque d'ID de l'appareil que vous souhaitez trouver. Le masque par défaut est *, qui représente tous les appareils.
Recherche sur les appareils	Cliquez sur ce bouton pour que l'application lance une recherche d'appareils selon les paramètres indiqués. Les résultats de la recherche sont repris dans le tableau inférieur.
Liste des appareils détectés	Ce tableau contient les colonnes suivantes : • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé. • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **Nom de l'appareil** : nom de l'appareil trouvé. • **ID de l'appareil** : identifiant de l'appareil trouvé.

Fenêtre Liste des appareils en fonction des événements du Contrôle des appareils

Dans cette fenêtre, vous pouvez créer une liste des appareils détectés lors des événements du Contrôle des appareils dans Kaspersky Security Center. Les appareils de cette liste peuvent ensuite être ajoutés à la liste des appareils de confiance.

Vous pouvez sélectionner un ou plusieurs appareils à ajouter à la liste des appareils de confiance.

Les informations sur les appareils sont disponibles si le Contrôle des appareils est activé, s'il existe une stratégie active et s'il y a eu une synchronisation avec l'Agent d'administration (fonctionne dans les limites spécifiées dans la stratégie de l'Agent d'administration, 15 minutes par défaut).

Lorsque vous créez une stratégie inactive, la liste sera vide.

Ajout d'appareils à partir de la liste des appareils détectés dans les événements de Kaspersky Security Center

Paramètre	Description
Types d'événements	Vous pouvez cocher les cases pour sélectionner les types d'événements du Contrôle des appareils envoyés à Kaspersky Security Center. La liste inclut les appareils détectés dans les événements du type spécifié. Toutes les cases sont cochées par défaut.
Groupe d'administration	Champ du saisie du nom du groupe d'administration contenant les appareils clients auxquels les appareils détectés sont connectés. La liste inclut uniquement les appareils connectés aux appareils clients du groupe d'administration spécifié. Vous pouvez spécifier une partie du nom du groupe. Par défaut, la liste inclut les appareils connectés aux appareils clients de n'importe quel groupe d'administration.
Période de formation des événements	Utilisez la liste déroulante pour sélectionner la période pendant laquelle les événements se sont produits. La liste inclut les appareils détectés dans les événements envoyés à Kaspersky Security Center pendant la période spécifiée. Par défaut, la liste inclut les appareils détectés dans les événements du mois dernier.
Recherche d'appareils	Cliquez sur ce bouton pour que l'application lance une recherche d'appareils selon les paramètres indiqués. Les résultats de la recherche sont repris dans le tableau inférieur.
Appareils trouvés	Ce tableau contient les colonnes suivantes : • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **ID de l'appareil** : identifiant de l'appareil trouvé. • **Nom de l'appareil** : nom de l'appareil trouvé. • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé. • **Date de connexion** : date à laquelle l'appareil détecté a été connecté. • **Groupe d'administration** : nom du groupe d'administration contenant l'appareil client auquel l'appareil détecté est connecté.
Commentaire	Champ de saisie de commentaires au sujet de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance (facultatif).
Autoriser l'accès aux utilisateurs et/ou aux groupes d'utilisateurs	Un champ qui affiche le nom de l'utilisateur et/ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé. La valeur par défaut est **\Everyone** (tous les utilisateurs).
Configurer	Cliquer sur le bouton ouvre la fenêtre Accès à un appareil de confiance.

Fenêtre Accès à un appareil de confiance

Dans cette fenêtre, vous pouvez configurer l'accès des utilisateurs ou des groupes d'utilisateurs à l'appareil de confiance sélectionné.

Accès à un appareil de confiance

Paramètre	Description
Utilisateurs et/ou groupes d'utilisateurs	Liste des utilisateurs et des groupes pour lesquels l'appareil ajouté sera approuvé. Par défaut, le tableau contient l'élément **\Tous** (tous les utilisateurs). Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier un utilisateur ou un groupe d'utilisateurs pour lesquels l'appareil sera approuvé.

Paramètres de l'appareil de confiance.

Paramètre	Description
Type	L'**Utilisateur** ou le **Groupe** pour lesquels l'appareil sera approuvé.
Utilisateur ou groupe	Le nom d'un utilisateur local ou de domaine (sans spécifier le nom complet avec le domaine, si le système permet de saisir des noms d'utilisateur dans ce format, ou dans le format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`) ou le nom d'un groupe d'utilisateurs pour lesquels l'appareil sera approuvé.

Fenêtre Type d'appareil

Cette fenêtre permet de configurer des modes d'accès pour différents types d'appareil.

Modes d'accès pour les types d'appareil

Paramètre	Description
Type d'appareil.	Types d'appareil (par exemple, Disques durs, Imprimantes).
Mode d'accès	Mode d'accès à l'appareil. Un clic droit sur la souris ouvre un menu contextuel dans lequel vous pouvez sélectionner l'une des options suivantes : • **Autoriser** pour octroyer l'accès aux appareils du type sélectionné. • **Bloquer** pour interdire l'accès aux appareils du type sélectionné. • **Dépend du bus** (valeur par défaut) pour autoriser ou interdire l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion. • **En fonction des règles** pour autoriser ou interdire l'accès aux appareils, selon une règle d'accès et sa planification. Cette option de menu est uniquement disponible pour les appareils de stockage (disques durs, lecteurs amovibles, disquettes, lecteurs CD/DVD). • **Lecture seule** : autoriser l'accès en lecture seule aux appareils du type sélectionné. Cette option de menu est uniquement disponible pour les appareils de stockage (disques durs, lecteurs amovibles, disquettes, lecteurs CD/DVD).

Vous pouvez configurer les règles et les horaires d'accès dans la fenêtre **Configuration de la règle d'accès aux appareils**, qui s'ouvre en double-cliquant sur le nom du type d'appareil.

Fenêtre Configuration de la règle d'accès aux appareils

Cette fenêtre permet configurer les règles d'accès et la planification pour les types d'appareil sélectionnés.

Pour ouvrir cette fenêtre, double-cliquez sur le nom du type d'appareil dans la fenêtre **Type d'appareil**.

Règles et planifications d'accès aux appareils

Paramètre	Description
Utilisateurs et/ou groupes d'utilisateurs	Liste des utilisateurs et des groupes pour lesquels vous pouvez configurer des planifications d'accès. Par défaut, le tableau contient l'élément **\Tous** (tous les utilisateurs). Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.
Règles d'accès aux appareils	Ce tableau contient les planifications d'accès pour les utilisateurs et les groupes d'utilisateurs. Il comporte les colonnes suivantes : • **Planification d'accès** : noms des planifications d'accès en vigueur. La case à côté de la planification indique si cette planification est utilisée par le module. • **Accès** : type d'accès pour la planification : **Autoriser** (octroyer l'accès aux appareils du type sélectionné) ou **Bloquer** (interdire l'accès aux appareils du type sélectionné). Vous pouvez configurer des planifications uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs CD/DVD. Le tableau contient par défaut une planification d'accès intitulée **Par défaut**. Celle-ci garantit l'accès intégral aux appareils pour tous les utilisateurs (sélection de l'option **\Tous** dans la liste **Utilisateurs et/ou groupes d'utilisateurs**) à tout moment, même si l'accès via le bus de connexion est autorisé pour ce type d'appareil. Vous pouvez ajouter, modifier et supprimer des planifications d'accès pour les utilisateurs sélectionnés. Il est impossible de modifier ou de supprimer la planification **Par défaut**.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier l'utilisateur ou le groupe d'utilisateurs auquel s'applique la règle d'accès à l'appareil.

Configuration de la règle d'accès aux appareils

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Nom d'utilisateur local ou nom du groupe d'utilisateurs auquel la règle s'applique.

Fenêtre Planification d'accès

Cette fenêtre permet de configurer les planifications d'accès aux appareils.

Planifier l'accès aux appareils

Paramètre	Description
Nom	Champ de saisie du nom de la planification d'accès.
Intervalles de temps	Tableau qui permet de préciser des intervalles de temps pour la planification (jours et heures). Les intervalles surlignés en vert sont inclus dans la planification. Pour exclure un intervalle de la planification, cliquez sur les cellules correspondantes. Les intervalles exclus de la planification sont surlignés en gris. Par défaut, tous les intervalles (24/7) sont inclus dans la planification.

Fenêtre Bus de connexion

Cette fenêtre permet de configurer le mode d'accès pour les bus de connexion.

Mode d'accès pour les bus de connexion

Paramètre	Description
Bus de connexion	Le bus de connexion via lequel les appareils sont connectés à l'appareil client : • **FireWire** • **USB**
Mode d'accès	Mode d'accès pour les bus de connexion. Un clic droit sur la souris ouvre un menu contextuel dans lequel vous pouvez sélectionner l'une des options suivantes : • **Autoriser** (valeur par défaut) permet d'accéder aux appareils connectés à l'aide de ce bus de connexion. • **Bloquer** : refuser l'accès aux appareils connectés via ce bus de connexion.

Contrôle Internet

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle Internet dans les propriétés de la stratégie (**Contrôles de sécurité → Contrôle Internet**).

Paramètres du module Contrôle Internet

Paramètre	Description
Activer le Contrôle Internet	La case active le module Contrôle Internet. La case est décochée par défaut.

Paramètres du Contrôle Internet	Le tableau contient une liste de règles d'accès aux ressources Web. Pendant le fonctionnement, le Contrôle Internet applique les règles dans l'ordre dans lequel elles sont répertoriées dans le tableau.
	Ce tableau contient les colonnes suivantes :
	• **État**. État de fonctionnement de la règle d'accès aux ressources Web :
	  • *Activé* : la règle est activée, le Contrôle Internet applique cette règle pendant son fonctionnement.
	  • *Désactivé* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle Internet.
	  Vous pouvez cocher ou décocher la case dans le tableau, et vous pouvez cocher ou décocher la case **Utiliser cette règle** dans la fenêtre **Règle du Contrôle Internet**.
	• **Action**. L'action que l'application entreprendra lorsqu'elle détectera une tentative d'accès aux ressources Web qui correspond à la règle.
	• **Nom**. Le nom de la règle d'accès aux ressources Web.
	Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.
	Vous pouvez également importer la liste des règles d'un fichier à l'aide du bouton **Avancé → Importer** et exporter la liste des règles ajoutées vers un fichier à l'aide du bouton **Avancé → Exporter les éléments sélectionnés** ou **Avancé → Tout exporter**. Lors de l'importation, vous serez invité à remplacer la liste des règles ou à ajouter des règles à une liste existante.

Règle par défaut	Dans la liste déroulante, vous pouvez sélectionner une règle par défaut, selon laquelle l'application régulera l'accès aux ressources Web qui ne sont pas soumises à d'autres règles : • **Autoriser**(valeur par défaut) : autoriser l'accès aux ressources Web. • **Bloquer** : bloque l'accès aux ressources Web.
Modèles de messages	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Modèles de messages**.

Fenêtre Règle du Contrôle Internet

Dans cette fenêtre, vous pouvez configurer les paramètres de la règle d'accès aux ressources Web.

Ajout d'une règle du Contrôle Internet

Paramètre	Description
Nom de la règle	Champ de saisie du nom de la règle d'accès aux ressources Web. Le nom de la règle doit être unique.
Utiliser cette règle	La case à cocher active ou désactive l'utilisation de cette règle pendant l'exécution de l'application. Si la case est cochée, la règle est activée, le Contrôle Internet applique cette règle pendant le fonctionnement. Si la case n'est pas cochée, la règle est désactivée et n'est pas utilisée pendant l'exécution du Contrôle Internet. À l'avenir, vous pourrez activer l'utilisation de cette règle par le Contrôle Internet en cochant la case. La case est cochée par défaut.
Filtrer le contenu	Dans la liste déroulante, vous pouvez sélectionner un filtre de contenu de ressource Web : • **Ne pas filtrer**(valeur par défaut). Lorsque vous sélectionnez cet élément de liste, le filtre de contenu des ressources Web n'est pas utilisé. • **Par catégories de contenu**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les catégories de contenu**. • **Par catégories de types de données**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les catégories de types de données**. • **Par catégories de contenu et types de données**. Lorsque vous sélectionnez cet élément de liste, les boutons **Sélectionner** deviennent disponibles. Ces boutons permettent d'ouvrir des fenêtres dans lesquelles vous pouvez sélectionner les catégories nécessaires.
Filtrer les adresses	Dans la liste déroulante, vous pouvez sélectionner un filtre d'adresse de ressource Web : • **Toute adresse** (valeur par défaut). Lorsque cet élément de la liste est sélectionné, le filtre d'adresses des ressources Web n'est pas utilisé ; la règle du Contrôle Internet est appliquée à toutes les adresses des ressources Web. • **Adresses indiquées**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner des adresses** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner des adresses**, dans laquelle vous pouvez sélectionner les adresses des ressources Web nécessaires.

Paramètre	Description
Appliquer aux utilisateurs	Dans la liste déroulante, vous pouvez sélectionner les utilisateurs soumis à la règle d'accès aux ressources web : • **À tous les utilisateurs** (valeur par défaut). Lorsque cet élément de la liste est sélectionné, le filtre des utilisateurs n'est pas utilisé et la règle Contrôle Internet est appliquée à tous les utilisateurs. • **Aux utilisateurs sélectionnés**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner les utilisateurs** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les utilisateurs**.
Horaire des règles	Dans la liste déroulante, vous pouvez configurer le calendrier de la règle d'accès à une ressource Web : • **Toujours** (valeur par défaut). Lorsque vous sélectionnez cet élément de la liste, une règle d'accès personnalisée à une ressource Web est appliquée sans restriction de temps, c'est-à-dire à tout moment. • **<Nom de la planification>**. Lorsque vous sélectionnez cet élément de liste, les boutons **Supprimer** et **Modifier** deviennent disponibles, en cliquant sur lesquels vous pouvez supprimer ou configurer ce calendrier. • **Ajouter un nouvelle planification**. Lorsque vous sélectionnez cet élément de liste, la fenêtre **Planification d'accès** s'ouvre, dans laquelle vous pouvez configurer un nouveau calendrier de fonctionnement de la règle d'accès à la ressource Web.
Action de la règle	Dans la liste déroulante, vous pouvez sélectionner l'action que le Contrôle Internet effectuera lorsqu'il détectera une tentative d'accès à une ressource Web qui correspond à la règle : • **Autoriser**(valeur par défaut) : autoriser l'accès à la ressource Web. • **Bloquer** : bloquer l'accès à la ressource Web et afficher un message concernant le refus d'accès. • **Informer** : afficher un avertissement indiquant que la ressource Web n'est pas recommandée à la visite. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.

Fenêtre Sélectionner les catégories de contenu

Dans cette fenêtre, vous pouvez sélectionner les catégories de contenu dont vous souhaitez contrôler l'accès.

Pour ce faire, cochez les cases à côté des catégories souhaitées.

Toutes les cases sont décochées par défaut.

Lorsque vous cochez les cases en regard de toutes les catégories de sous-contenu, la case en regard de la catégorie de contenu principale qui contient les sous-catégories n'est pas automatiquement sélectionnée.

Fenêtre Sélectionner les catégories de type de données

Cette fenêtre vous permet de sélectionner les catégories de types dont vous souhaitez contrôler l'accès.

Pour ce faire, cochez les cases à côté des catégories souhaitées.

Toutes les cases sont décochées par défaut.

Fenêtre Sélectionner les adresses

Dans cette fenêtre, vous pouvez spécifier les adresses des ressources Web auxquelles vous souhaitez contrôler l'accès des utilisateurs. Vous pouvez spécifier plusieurs adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie. Vous pouvez utiliser des masques pour spécifier des adresses.

Si vous souhaitez spécifier un groupe d'adresses, ouvrez la fenêtre **Sélectionner des groupes d'adresses**, en cliquant sur le bouton **Ajouter un groupe d'adresses**.

Fenêtre Sélectionner un groupe d'adresses

Le tableau contient des groupes d'adresses de ressources Web auxquelles l'accès des utilisateurs est contrôlé par le module Contrôle Internet.

Si vous souhaitez ajouter un groupe d'adresses à la liste des groupes dans la fenêtre **Sélectionner les adresses**, cochez la case en regard du nom du groupe dans le tableau et cliquez sur le bouton **Ajouter** situé sous le tableau.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Si vous souhaitez ajouter un nouveau groupe d'adresses à la liste des groupes de cette fenêtre, ouvrez la fenêtre **Ajout d'un groupe d'adresses** en cliquant sur le bouton **Ajouter** situé au-dessus du tableau.

Par défaut, le tableau est vide.

Fenêtre Ajout d'un groupe d'adresses

Dans cette fenêtre, vous pouvez spécifier des groupes d'adresses de ressources Web auxquels vous souhaitez contrôler l'accès des utilisateurs. Vous pouvez spécifier plusieurs adresses dans un groupe d'adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie. Vous pouvez utiliser des masques pour spécifier des adresses.

Fenêtre Sélectionner les utilisateurs

Le tableau contient les noms et les groupes d'utilisateurs pour lesquels l'accès aux ressources Web est contrôlé conformément à la règle.

Vous pouvez ajouter, modifier ou supprimer des éléments dans le tableau

Si vous souhaitez ajouter un nouvel utilisateur et/ou groupe d'utilisateurs à la liste des utilisateurs de cette fenêtre, en cliquant sur le bouton **Ajouter** situé au dessus du tableau, ouvrez la fenêtre **Utilisateur ou groupe**.

Par défaut, le tableau est vide.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier l'utilisateur ou le groupe d'utilisateurs auquel s'applique la règle d'accès aux ressources Web.

Configuration des règles d'accès aux ressources Web

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle s'applique.

Fenêtre Planification d'accès

Dans cette fenêtre, vous pouvez configurer le calendrier d'accès aux ressources Web.

Calendrier d'accès aux ressources Web

Paramètre	Description
Nom	Champ de saisie du nom de la planification d'accès.
Intervalles de temps	Tableau qui permet de préciser des intervalles de temps pour la planification (jours et heures). Les intervalles surlignés en vert sont inclus dans la planification. Pour exclure un intervalle de la planification, cliquez sur les cellules correspondantes. Les intervalles exclus de la planification sont surlignés en gris. Par défaut, tous les intervalles (24/7) sont inclus dans la planification.

Contrôle des applications

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle des applications dans les propriétés de la stratégie (**Contrôles de sécurité** → **Contrôle des applications**).

Paramètres du module Contrôle des applications

Paramètre	Description
Activer le module Contrôle des applications	Cette case permet d'activer le module Contrôle des applications. La case est décochée par défaut.
Action à réaliser en cas de tentative de lancement de l'application	Action que Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles configurées : • **Appliquer les règles** (valeur par défaut). Si vous choisissez cette option, l'application Kaspersky Endpoint Security applique les règles du Contrôle des applications et exécute l'action définie. • **Tester les règles**. Lorsque vous sélectionnez cette option, Kaspersky Endpoint Security teste les règles et génère un événement concernant une tentative de lancement d'une application qui correspond aux règles.
Mode Contrôle des applications	Mode de fonctionnement du module Contrôle des applications : • **Liste d'autorisation**. Si vous choisissez cette option, l'application Kaspersky Endpoint Security interdit à tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. • **Liste de refus** (valeur par défaut). Si vous choisissez cette option, l'application Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.
Règles du Contrôle des **applications**	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre Règles du Contrôle des applications.
Application des règles	Dans la liste déroulante, vous pouvez choisir comment ajouter des règles : • **Remplacer les règles locales par les règles depuis la stratégie**. Lorsque vous sélectionnez cet élément de la liste, l'application applique uniquement les règles spécifiées dans la stratégie. • **Ajouter des règles depuis la stratégie aux règles locales** (valeur par défaut). Si vous choisissez cette option, l'application applique les règles configurées dans la stratégie en même temps que les règles locales configurées sur l'appareil protégé.

Fenêtre Règles du Contrôle des applications

Le tableau **Règles du Contrôle des applications** contient les règles utilisées par le module Contrôle des applications. Par défaut, le tableau des règles du contrôle des applications est vide.

Paramètres des règles du contrôle des applications

Paramètre	Description
nom de la catégorie ;	Le nom de la catégorie des applications qui est utilisée par la règle.
État	État de fonctionnement de la règle du Contrôle des applications. • *Activé* : la règle est activée, le Contrôle des applications applique cette règle pendant son fonctionnement. • *Inactif* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle des applications. • *Essai* : le Contrôle des applications autorise le lancement des applications qui satisfont aux conditions de la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport. Vous pouvez modifier l'état d'une règle dans la fenêtre **Ajouter une nouvelle règle**.

Vous pouvez ajouter, modifier et supprimer des règles de contrôle des applications.

Fenêtre Ajouter une nouvelle règle

Cette fenêtre permet de configurer les paramètres de la règle du Contrôle des applications.

Ajout de la règle du Contrôle des applications

Paramètre	Description
Description	Description de la règle du Contrôle des applications.
État de la règle	La liste déroulante permet de sélectionner l'état du fonctionnement des règles du contrôle des applications : • *Activé* : la règle est activée, le Contrôle des applications applique cette règle pendant son fonctionnement. • *Inactif* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle des applications. • *Essai* : le Contrôle des applications autorise le lancement des applications qui satisfont aux conditions de la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.
Catégorie	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Catégories des applications**.
Utilisateurs et leurs droits	Le tableau contient une liste d'utilisateurs ou de groupes d'utilisateurs auxquels s'applique la règle de contrôle des applications ainsi que les types d'accès qui leur sont attribués et il se compose des colonnes suivantes : • **Nom d'utilisateur ou de groupe** : les noms d'utilisateurs ou les noms de groupes d'utilisateurs affectés par la règle de contrôle des applications. • **Accès** : type d'accès : **Autoriser** l'exécution des applications ou **Bloquer** leur exécution. Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.

Fenêtre Catégories d'applications

Cette fenêtre vous permet d'ajouter une nouvelle catégorie ou de configurer les paramètres de catégorie pour une règle du Contrôle des applications.

L'utilisation des catégories KL de l'application Kaspersky Security Center n'est pas prise en charge par l'application Kaspersky Endpoint Security.

Catégories du Contrôle des applications

Paramètre	Description
nom de la catégorie ;	Liste des catégories du Contrôle des applications ajoutées.
Ajouter	Cliquez sur ce bouton pour lancer l'assistant de création d'une catégorie. Suivez les instructions de l'Assistant. Pour plus d'informations sur la création d'une catégorie, consultez l'aide de Kaspersky Security Center.
Modifier	Cliquez sur le bouton pour ouvrir la fenêtre des propriétés des catégories qui permet de modifier les paramètres des catégories. La catégorie **Golden Image (locale)** ne peut pas être modifiée.

Fenêtre Utilisateur ou groupe

Cette fenêtre permet d'indiquer l'utilisateur local ou de domaine ou le groupe d'utilisateurs pour lequel vous souhaitez configurer la règle.

Ajout de la règle du Contrôle des applications

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.
Accès	Type d'accès : **Autoriser** le lancement des applications ou **Bloquer** le lancement des applications.

Inventaire

Dans la Console d'administration de Kaspersky Security Center, vous pouvez effectuer un inventaire des applications sur l'appareil protégé à l'aide de la tâche *Inventaire*.

Vous pouvez créer et lancer des tâches d'Inventaire définies par l'utilisateur. Vous pouvez gérer les paramètres d'analyse en modifiant les paramètres des tâches.

Les bases de données de l'application Kaspersky Security Center peuvent conserver les informations relatives à 150 000 fichiers traités. Une fois ce chiffre atteint, les nouveaux fichiers ne seront pas traités. Afin de rétablir le fonctionnement de la tâche d'inventaire, il convient de supprimer sur l'appareil doté de l'application Kaspersky Endpoint Security tous les fichiers comptabilisés antérieurement dans la base de données de Kaspersky Security Center suite à l'analyse de l'inventaire.

Paramètres de la tâche d'inventaire

Paramètre	Description
Action avec la catégorie Golden Image une fois la tâche terminée	Dans la liste déroulante, vous pouvez sélectionner l'action que Kaspersky Endpoint Security doit effectuer sur la catégorie d'applications Golden Image à la fin de la tâche Inventaire : • **Laisser inchangé** – ne pas modifier la catégorie d'applications Golden Image une fois l'inventaire terminé. Cette valeur est sélectionnée par défaut. • **Mettre à jour ou créer (si elle n'existe pas)** – ajouter à la catégorie d'applications Golden Image les applications que la tâche Inventaire découvre sur l'appareil. Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. • **Supprimer** – vider la catégorie d'applications Golden Image. La catégorie est effacée dès le lancement de la tâche, sans effectuer d'inventaire des fichiers sur l'appareil. Vous pouvez utiliser la catégorie d'applications Golden Image dans les règles du Contrôle des applications.
Analyser tous les fichiers exécutables	La case active ou désactive l'analyse des fichiers exécutables. La case est cochée par défaut.
Analyser les fichiers binaires	La case active ou désactive l'analyse des fichiers binaires (avec l'extension .elf, .java et .pyc). La case est cochée par défaut.
Analyser les scripts	La case active ou désactive l'analyse des scripts. La case est cochée par défaut.
Zones d'inventaire	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'analyse**.

La section **Exclusions** de la tâche Inventaire permet de configurer les zones d'exclusion de l'analyse.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse : /usr/bin.

Paramètres de la zone d'analyse de la tâche Inventaire

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de modifier une zone d'analyse pour la tâche Inventaire.

Paramètres de la zone d'inventaire

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre Zones d'analyse. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant l'exécution de la tâche. Si la case est cochée, l'application traite cette zone d'analyse au moment de l'exécution de la tâche. Si cette case est décochée, l'application ne traite pas cette zone d'analyse au moment de l'exécution de la tâche. Par la suite, vous pouvez inclure cette zone dans les paramètres de la tâche en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'analyse. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ ne peut être vide.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution de la tâche. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Section Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre Zones d'exclusion. Cette fenêtre permet de définir la liste des zones d'exclusion du contrôle.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion de l'analyse pour la tâche Inventaire.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'exclusion de cette zone pendant l'exécution de la tâche. Si cette case est cochée, l'application exclut cette zone au moment de l'exécution de la tâche. Si cette case est décochée, l'application inclut cette zone au moment de l'exécution de la tâche. Par la suite, vous pouvez exclure cette zone de l'analyse après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion d'inventaire. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ ne peut être vide.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Contrôle de l'intégrité du système

Dans la Console d'administration, vous pouvez configurer les paramètres du Contrôle de l'intégrité du système dans les propriétés de la stratégie (**Contrôles de sécurité → Contrôle de l'intégrité du système**).

Paramètres du Contrôle de l'intégrité du système

Paramètre	Description
Activer le Contrôle de l'intégrité du système	La case active ou désactive le module Contrôle de l'intégrité du système. La case est décochée par défaut.
Zones de contrôle	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'analyse**.
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**.

Fenêtre Zones d'analyse

Le tableau contient les zones de contrôle pour le module Contrôle de l'intégrité du système. L'application contrôle les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone de contrôle **Objets internes de Kaspersky** (/opt/kaspersky/kesl/).

Paramètres Zones de contrôle

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la Zones de contrôle.
Chemin	Chemin au répertoire que l'application protège.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer des zones de contrôle pour le module du Contrôle de l'intégrité du système.

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone de contrôle. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application contrôle cette zone de contrôle pendant le fonctionnement de l'application. Si cette case est décochée, l'application ne contrôle pas cette zone de contrôle pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone de contrôle. Le champ ne peut être vide. Le chemin /opt/kaspersky/kesl est défini par défaut.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion du contrôle pour le module Contrôle de l'intégrité du système. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu du contrôle.
État	L'état indique si l'application exclut cette zone de l'analyse lorsque la tâche est exécutée.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer une liste des zones d'exclusion à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones d'exclusion vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones d'exclusion ou à ajouter des zones d'exclusion à une liste existante.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion du contrôle pour le module Contrôle de l'intégrité du système.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone de surveillance pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone du contrôle pendant le fonctionnement du module. Si cette case est décochée, l'application ne contrôle pas cette zone pendant le fonctionnement du module. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion. Le champ ne peut être vide. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Masques	La liste contient les masques des noms des objets exclus de la surveillance par l'application. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de la surveillance. Exemples : Le masque `*.txt` fait référence à tous les fichiers texte. Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets du contrôle, en fonction d'un masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de la surveillance.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Vérification de l'intégrité du système

Dans la Console d'administration, vous pouvez vérifier l'intégrité du système à l'aide de la tâche *Vérification de l'intégrité du système*.

Vous pouvez créer et lancer des tâches personnalisées de vérification de l'intégrité du système. Vous pouvez gérer les paramètres d'analyse en modifiant les paramètres des tâches.

Dans la section **Paramètres** dans les propriétés de la tâche Vérification de l'intégrité du système, vous pouvez configurer les paramètres indiqués dans le tableau ci-dessous.

Paramètres de la tâche Vérification de l'intégrité du système

Paramètre	Description
Actualiser l'instantané de l'état du système à chaque démarrage de la tâche	Cette case active ou désactive la recréation d'une ligne de base de système chaque fois que la tâche Vérification de l'intégrité du système est démarrée. La case est décochée par défaut.
Utiliser le hachage SHA256 pour l'analyse	La case active ou désactive l'utilisation du hachage du fichier comme critère de comparaison de l'état actuel du fichier avec l'état d'origine. Si la case n'est pas cochée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique). La case est décochée par défaut.
Surveiller les répertoires des zones de contrôle	La case active ou désactive la vérification des répertoires dans les zones de surveillance spécifiées lors des vérifications de l'intégrité du système. La case est décochée par défaut.
Surveiller l'heure du dernier accès au fichier	Cette case active ou désactive le suivi du temps d'accès au fichier pendant l'exécution de la vérification de l'intégrité du système. La case est décochée par défaut.
Zones de contrôle	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre Zones d'analyse.

Dans les sections **Zones d'exclusion** des propriétés de la Vérification de l'intégrité du système, vous pouvez définir des exclusions de la surveillance et des exclusions d'après le masque.

Fenêtre Zones d'analyse

Le tableau contient les zones de contrôle pour la tâche Vérification de l'intégrité du système. L'application contrôle les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone de contrôle **Objets internes de Kaspersky** (/opt/kaspersky/kesl/).

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone	Nom de la Zones de contrôle.
Chemin	Chemin au répertoire que l'application protège.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer des zones de surveillance pour la tâche Vérification de l'intégrité du système.

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone de contrôle. Ce nom sera affiché dans le tableau de la fenêtre Zones d'analyse. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application contrôle cette zone de contrôle pendant le fonctionnement de l'application. Si cette case est décochée, l'application ne contrôle pas cette zone de contrôle pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone de contrôle. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ ne peut être vide. Le chemin /opt/kaspersky/kesl est défini par défaut.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Section Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre Zones d'exclusion. Cette fenêtre permet de définir la liste des zones d'exclusion du contrôle.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre Exclusions d'après le masque. Cette fenêtre permet de configurer l'exclusion des objets du contrôle sur la base d'un masque de nom.

Fenêtre Zones d'exclusion

Le tableau contient les zones d'exclusion de l'analyse pour la tâche Vérification de l'intégrité du système. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau est vide.

Paramètres de la zone d'exclusion de l'analyse de la tâche Vérification de l'intégrité du système

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si l'application exclut cette zone de l'analyse lorsque la tâche est exécutée.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion du contrôle pour la tâche Vérification de l'intégrité du système.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone de surveillance pendant le fonctionnement de l'application. Si cette case est cochée, l'application exclut cette zone du contrôle lorsque la tâche est exécutée. Si cette case est décochée, l'application ne contrôle pas cette zone lorsque la tâche est exécutée. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion. Vous pouvez utiliser des masques pour spécifier le chemin. Le champ ne peut être vide. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Masques	La liste contient les masques des noms des objets exclus de la surveillance par l'application. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse. Exemples : Le masque `*.txt` fait référence à tous les fichiers texte. Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets du contrôle, en fonction d'un masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Tâches locales

Gestion de la tâche

Dans la Console d'administration, vous pouvez configurer l'autorisation d'afficher et de gérer les tâches dans les propriétés de la stratégie (**Tâches locales** → **Gestion de la tâche**).

Paramètres de gestion des tâches

Paramètre	Description
Autoriser l'utilisation des tâches locales	La case permet d'autoriser ou non l'utilisateur à consulter les tâches locales créées dans l'application Kaspersky Endpoint Security et à les gérer sur les appareils clients administrés. Si cette case est cochée, les utilisateurs peuvent configurer et exécuter des tâches dans l'interface graphique de l'application et dans la ligne de commande. Si la case est décochée, l'utilisation des tâches locales est arrêtée. Les tâches locales ne s'exécutent pas selon le calendrier prévu. Les tâches ne sont pas disponibles pour le lancement et la configuration dans l'interface graphique de l'application ou dans la ligne de commande. La case est décochée par défaut.
Autoriser à consulter et à administrer les tâches créées via KSC	La case permet ou non aux utilisateurs de visualiser les tâches créées via Kaspersky Security Center et d'administrer ces tâches sur les appareils clients. Si la case est cochée, les tâches créées via Kaspersky Security Center s'affichent dans l'interface graphique de l'application. Les utilisateurs peuvent démarrer et arrêter ces tâches à partir de l'interface graphique de l'application et dans la ligne de commande. Si la case est décochée, l'affichage et la gestion des tâches créées via Kaspersky Security Center ne sont pas disponibles dans l'interface graphique de l'application ni dans la ligne de commande. La case est décochée par défaut.

Protection contre les menaces avancées et les attaques ciblées

Intégration avec la solution Kaspersky Managed Detection and Response

Dans la Console d'administration, vous pouvez activer ou désactiver le module MDR et télécharger le fichier BLOB MDR dans les propriétés de la stratégie (**Detection and Response → Managed Detection and Response**).

Paramètres d'intégration à MDR

Paramètre	Description
Activer Managed Detection and Response	Le case active ou désactive le module MDR, nécessaire pour intégrer l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response. Le module est désactivé par défaut. Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, vous serez invité à accepter les conditions d'utilisation de Kaspersky Security Network pour activer Kaspersky Security Network en mode avancé. Si la modification des paramètres KSN est interdite par la stratégie parent, un message d'erreur s'affiche et le module MDR n'est pas activé.
Charger	En appuyant sur le bouton, vous ouvrez une fenêtre standard de Microsoft Windows dans laquelle vous pouvez sélectionner le fichier MDR BLOB à télécharger. Cette action est obligatoire si vous avez des tenants ou si vous avez activé le module MDR à l'aide du fichier BLOB MDR.

Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR, inclus avec la solution Kaspersky Managed Detection and Response.

En chargeant le fichier BLOB, vous acceptez de transférer automatiquement les données de l'appareil sur lequel Kaspersky Endpoint Security est installé à Kaspersky à des fins de traitement. Ne chargez pas le fichier si vous n'acceptez pas le traitement des données transférées. Pour une description détaillée des données transmises, consultez l'aide de Kaspersky Managed Detection and Response.

Intégration de Kaspersky Endpoint Detection and Response (on-premises)

Dans la Console d'administration, vous pouvez activer ou désactiver le module EDR Expert (on-premises) et gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Endpoint Detection and Response (KATA) dans les propriétés de la stratégie (**Detection and Response → EDR Expert (on-premises)**).

Si l'option **Endpoint Detection and Response Expert (version 8.0 et supérieure)** est sélectionnée dans Web Console pour le module EDR Expert (on-premises), c'est-à-dire si le mode d'intégration EDR Expert (on-premises) est sélectionné, un avertissement s'affiche dans la Console d'administration et les paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA) ne sont pas disponibles. Vous pouvez modifier le mode d'intégration dans Web Console.

Paramètres de l'intégration de Kaspersky Endpoint Detection and Response (on-premises)

Paramètre	Description
Activer Endpoint Detection and Response Expert (on-premises)	Cette case active ou désactive le module EDR Expert (on-premises), qui assure l'intégration avec Kaspersky Endpoint Detection and Response (KATA). Le module est désactivé par défaut.
Activer la prévention du lancement des objets	Cette case active ou désactive les règles EDR Expert (on-premises) de prévention de l'exécution des objets.
Serveurs KATA	Cliquer sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer la connexion aux serveurs KATA, ainsi qu'afficher la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion aux serveurs	Cliquez sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs KATA, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs KATA.
Paramètres de transfert des données	Le bouton **Configurer** ouvre une fenêtre dans laquelle vous pouvez configurer les paramètres de transfert des données aux serveurs KATA.

Configuration de connexion aux serveurs KATA

Le tableau affiche une liste des paramètres de connexion aux serveurs KATA. Pour chaque serveur auquel une connexion est configurée, le tableau indique l'adresse IP du serveur (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) et le port.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur KATA.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Paramètres de connexion au serveur

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur KATA, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur. Valeur par défaut : `127.0.0.1`.
Port	Port de connexion au serveur KATA. Valeur par défaut : `443`.

+-/Configuration des paramètres généraux de connexion aux serveurs KATA

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs KATA.

Paramètres de connexion au serveur KATA

Paramètre	Description
Envoyer une demande de synchronisation au serveur KATA toutes les (minutes)	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur KATA, en minutes. Valeur par défaut : `5`.
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur KATA en secondes. Valeur par défaut : `10`.

Paramètre	Description
Durée d'attente maximale de la réponse du serveur (en secondes)	Durée maximale d'attente de la réponse du serveur KATA en secondes. Valeur par défaut : `10`.
Autoriser l'envoi de télémétrie	Active ou désactive l'envoi de données d'événement sur les appareils (télémétrie) au serveur KATA. La télémétrie est activée par défaut.

Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur :
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
	Dans la fenêtre d'ajout un certificat, vous pouvez ajouter un certificat du serveur KATA de l'une des manières suivantes :
	  • Dans le champ **Ajouter à partir d'un fichier**, spécifiez le chemin d'accès au fichier de certificat contenant le certificat au format DER ou PEM. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier.
	  • Copier le contenu du fichier de certificat dans le champ **Saisir les données du certificat**.
	Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.
	• **Supprimer** : supprime un certificat du serveur ajouté précédemment. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.

Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes :
	• **Utiliser la vérification en deux étapes** : active ou désactive l'utilisation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur KATA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client.
	  L'authentification bidirectionnelle doit être activée du côté du serveur KATA.
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat client pour sécuriser davantage la connexion au serveur KATA. Le bouton apparaît si la case **Utiliser la vérification en deux étapes** est cochée et que le certificat client n'a pas encore été ajouté.
	Pour ajouter un certificat client, dans la fenêtre d'ajout d'un certificat, indiquez le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Saisissez ensuite le mot de passe du certificat client dans le champ **Mot de passe du conteneur crypto**.
	  Ce champ est obligatoire. Un message d'erreur s'affiche si vous essayez d'enregistrer les paramètres sans saisir de mot de passe.
	Si le mot de passe est correct, le bouton **OK** devient actif. Vous pouvez enregistrer les paramètres.
	• **Supprimer** : supprime le certificat client précédemment ajouté. Le bouton s'affiche uniquement si le certificat client a été ajouté.

Configuration des paramètres du transfert des données aux serveurs KATA

Cette fenêtre permet de configurer les paramètres de connexion au serveur KATA.

Paramètres de transfert des données aux serveurs KATA

Paramètre	Description
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur KATA. Valeur par défaut : `30`.
Activer la régulation du nombre d'événements	Active ou désactive la limitation du nombre d'événements envoyés au serveur KATA.

Paramètre	Description
Nombre maximum d'événements par heure.	Nombre maximum d'événements par heure. Valeur par défaut : `3000`.
Pourcentage d'événements dépassant la limite	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type (par exemple, les événements de changement de registre) et le nombre total d'événements dépasse la limite définie en pourcentage. Valeur par défaut : `15`.

Intégration avec Kaspersky Network Detection and Response (KATA)

Dans la Console d'administration, vous pouvez activer ou désactiver le module NDR (KATA) et gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Network Detection and Response (KATA) dans les propriétés de la stratégie (**Detection and Response → Network Detection and Response (KATA)**).

Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)

Paramètre	Description
Activer Network Detection and Response (KATA)	La case active ou désactive le module NDR (KATA). Le module est désactivé par défaut.
Serveurs NDR	Cliquer sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer la connexion aux serveurs NDR, ainsi qu'afficher la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion au serveur	Cliquez sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs NDR, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs NDR.
Paramètres de transfert des données	Le bouton **Configurer** ouvre une fenêtre dans laquelle vous pouvez configurer les paramètres de transfert des données aux serveurs NDR.

Configuration de connexion aux serveurs NDR

Le tableau affiche une liste des paramètres de connexion aux serveurs NDR. Pour chaque serveur auquel une connexion est configurée, le tableau indique l'adresse IP du serveur (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) et le port.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur NDR.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Paramètres de connexion au serveur

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur NDR, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Valeur par défaut : `127.0.0.1`.
Port	Port de connexion au serveur NDR. Valeur par défaut : `443`.

+-/Configuration des paramètres généraux de connexion aux serveurs NDR

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs NDR.

Paramètres de connexion au serveur NDR

Paramètre	Description
Envoyer une demande de synchronisation au serveur NDR toutes les (minutes)	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en minutes. Valeur par défaut : `5`.
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur NDR en secondes. Valeur par défaut : `10`.
Durée d'attente maximale de la réponse du serveur (en secondes)	Durée maximale d'attente de la réponse du serveur NDR en secondes. Valeur par défaut : `10`.

Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur :
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
	Dans la fenêtre d'ajout d'un certificat, vous pouvez ajouter un certificat du serveur NDR de l'une des manières suivantes :
	  • Dans le champ **Ajouter à partir d'un fichier**, spécifiez le chemin d'accès au fichier de certificat contenant le certificat au format DER ou PEM. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier.
	  • Copier le contenu du fichier de certificat dans le champ **Saisir les données du certificat**.
	Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.
	• **Supprimer** : supprime un certificat du serveur ajouté précédemment. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.

Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes :
	• **Utiliser la vérification en deux étapes** : active ou désactive l'utilisation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur NDR. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client.
	  L'authentification bidirectionnelle doit être activée du côté du serveur NDR.
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat client pour sécuriser davantage la connexion au serveur NDR. Le bouton apparaît si la case **Utiliser la vérification en deux étapes** est cochée et que le certificat client n'a pas encore été ajouté.
	Pour ajouter un certificat client, dans la fenêtre d'ajout d'un certificat, indiquez le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Saisissez ensuite le mot de passe du certificat client dans le champ **Mot de passe du conteneur crypto**.
	  Ce champ est obligatoire. Un message d'erreur s'affiche si vous essayez d'enregistrer les paramètres sans saisir de mot de passe.
	Si le mot de passe est correct, le bouton **OK** devient actif. Vous pouvez enregistrer les paramètres.
	• **Supprimer** : supprime le certificat client précédemment ajouté. Le bouton s'affiche uniquement si le certificat client a été ajouté.

Configuration des paramètres du transfert des données aux serveurs NDR

Cette fenêtre permet de configurer les paramètres de connexion au serveur NDR.

Paramètres de transfert des données aux serveurs NDR

Paramètre	Description
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur NDR. Valeur par défaut : `30`.
Nombre maximum d'événements dans un paquet	Nombre maximum d'événements dans un paquet. Valeur par défaut : `1024`.
Fréquence d'interrogation des serveurs	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en secondes. Valeur par défaut : `450`.
Activer la régulation du nombre d'événements	Active ou désactive la limitation du nombre d'événements envoyés au serveur NDR.
Nombre maximum d'événements par heure.	Nombre maximum d'événements par heure. Valeur par défaut : `3000`.
Pourcentage d'événements dépassant la limite	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type (par exemple, les événements de changement de registre) et le nombre total d'événements dépasse la limite définie en pourcentage. Valeur par défaut : `15`.

Intégration avec KUMA

Dans la Console d'administration, vous pouvez activer ou désactiver l'intégration de Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform et gérer les paramètres d'intégration dans les propriétés de la stratégie (**Intégration KUMA** → **Intégration KUMA**).

Paramètres d'intégration avec Kaspersky Unified Monitoring and Analysis Platform

Paramètre	Description
Activer l'intégration avec KUMA	Active ou désactive l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Unified Monitoring and Analysis Platform. Par défaut, l'intégration avec KUMA est désactivée.
Utiliser une connexion chiffrée	La case active ou désactive l'utilisation de l'analyse du certificat du serveur pour sécuriser davantage la connexion au serveur KUMA. Pour vérifier le certificat du serveur, vous devez cocher cette case et ajouter le certificat du serveur dans la fenêtre Serveur KUMA. La case est décochée par défaut.
Serveurs KUMA	Le bouton **Configurer** ouvre la fenêtre Serveurs KUMA. Cette fenêtre permet de configurer la connexion aux serveurs KUMA, ainsi que visualiser la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion au serveur KUMA	Cliquez sur le bouton **Configurer** pour ouvrir la fenêtre Paramètres de connexion au serveur dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs KUMA, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs KUMA.
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur KUMA. Valeur par défaut : `30`.

Fenêtre Serveurs KUMA

Cette fenêtre affiche le tableau contenant les paramètres de connexion aux serveurs KUMA. Pour chaque serveur auquel une connexion est configurée, le tableau indique :

- L'adresse IP (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) du serveur. Si dans la fenêtre de configuration de l'intégration avec KUMA, vous avez cochez la case **Utiliser une connexion chiffrée**, vous devez spécifier le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat d'une licence pour utiliser KUMA.
- Port de connexion au serveur KUMA.
- Le protocole utilisé pour se connecter au serveur KUMA.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur KUMA.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Fenêtre Serveur KUMA

Dans cette fenêtre, vous pouvez spécifier les paramètres de connexion au serveur KUMA.

Paramètres de connexion au serveur KUMA

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur KUMA, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Si dans la fenêtre de configuration de l'intégration avec KUMA, vous avez cochez la case **Utiliser une connexion chiffrée**, vous devez spécifier le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat d'une licence pour utiliser KUMA.
Port	Port de connexion au serveur KUMA. Valeur par défaut : `443`.
Protocole.	Protocole de connexion au serveur KUMA : TCP, UDP ou HTTP/HTTPS avec compression. Lorsque vous sélectionnez le protocole UDP, l'utilisation de certificats pour la sécurité de la connexion n'est pas prise en charge et il n'y a aucun événement de connexion avec le serveur KUMA. Valeur par défaut : TCP.

Fenêtre Paramètres de connexion aux serveurs KUMA

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs KUMA.

Paramètres de connexion au serveur KUMA

Paramètre	Description
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur KUMA en secondes. Valeur par défaut : `5`.
Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur.
Ajouter (certificat du serveur)	Ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
Supprimer (certificat du serveur)	Supprime le certificat du serveur. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.
Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes.
Utiliser la vérification en deux étapes	La case active ou désactive l'utilisation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client. L'authentification bidirectionnelle doit être activée du côté du serveur KUMA.
Ajouter (certificat client)	Ouvre la fenêtre d'ajout d'un certificat client pour sécuriser la connexion au serveur KUMA. Le bouton s'affiche si le certificat client n'a pas encore été ajouté. Si vous souhaitez renforcer la sécurité de connexion, vous devez activer la validation des certificats client du côté du serveur KUMA et cocher la case **Utiliser la vérification en deux étapes** dans cette fenêtre.
Supprimer (certificat client)	Supprime le certificat client. Le bouton s'affiche uniquement si le certificat client a été ajouté.

Fenêtre d'ajout d'un certificat de serveur

Cette fenêtre permet d'ajouter un certificat du serveur KUMA de l'une des manières suivantes :

- Indiquer le chemin d'accès au fichier de certificat dans le champ **Ajouter à partir d'un fichier**. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Indiquer le chemin d'accès à un fichier contenant un certificat au format DER ou PEM.
- Copiez le contenu du fichier de certificat dans le champ **Saisir les détails du certificat**.

Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.

Fenêtre d'ajout d'un certificat client

Cette fenêtre permet d'ajouter un certificat client pour sécuriser davantage la connexion au serveur KUMA.

Si vous souhaitez renforcer la sécurité de connexion, vous devez activer la validation des certificats client du côté du serveur KUMA et cocher la case **Utiliser la vérification en deux étapes** dans la fenêtre **Paramètres de connexion aux serveurs KUMA**.

Pour ajouter un certificat client, indiquez le chemin d'accès au cryptocontainer (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Saisissez ensuite le mot de passe du certificat client dans le champ **Mot de passe du conteneur crypto**.

Ce champ est obligatoire. Un message d'erreur s'affiche si vous essayez d'enregistrer les paramètres sans saisir de mot de passe.

Si le mot de passe est correct, le bouton **OK** devient actif. Vous pouvez enregistrer les paramètres.

Quarantaine

Dans la Console d'administration, vous pouvez configurer les paramètres de la quarantaine dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres des stockages**) et dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres des stockages**).

Paramètres de quarantaine

Paramètre	Description
Limiter la taille de la quarantaine à (Mo)	La case active ou désactive la limitation de la taille maximale de la quarantaine par la valeur spécifiée (en mégaoctets). Si la case est décochée, la taille de la quarantaine est illimitée. Valeurs admises : 1 à 999999. La valeur par défaut est de 200 si l'application est utilisée en mode standard ou en mode EDR Agent, et de 100 si l'application est utilisée en mode Light Agent.
Notifier lorsque la quarantaine est pleine à (%)	La case active ou désactive la limite du pourcentage de plénitude de la quarantaine à laquelle un événement sur la plénitude de la quarantaine est généré. Si la case n'est pas cochée, l'événement de quarantaine complète n'est pas généré. Valeurs admises : 1 à 100. Valeur par défaut : 90.

Prévention de l'exécution des objets

Vous pouvez activer ou désactiver la prévention de l'exécution des objets dans la Console d'administration uniquement si l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA) est activée.

Vous pouvez activer ou désactiver la prévention de l'exécution des objets dans les propriétés de la stratégie (**Paramètres de l'application** → **Detection and Response** → **EDR Expert (on-premises)**).

La case à cocher **Activer la prévention du lancement des objets** sous **Prévention du lancement des objets** active ou désactive les règles EDR Expert (on-premises) de prévention de l'exécution des objets.

Paramètres généraux

Dans la Console d'administration, vous pouvez gérer les paramètres généraux de l'application qui définissent le fonctionnement de l'application dans son ensemble et celui de ses fonctions individuelles, dans les propriétés de la stratégie (**Paramètres généraux**).

Serveur Proxy

Dans la Console d'administration, vous pouvez gérer les paramètres du serveur proxy dans les propriétés de la stratégie (**Paramètres généraux → Paramètres du serveur proxy**).

Paramètres du serveur proxy

Paramètre	Description
Ne pas utiliser de serveur proxy	Si cette option est sélectionnée, le serveur proxy n'est pas utilisé dans le fonctionnement de l'application.
Utiliser les paramètres indiqués du serveur proxy	Si cette option est sélectionnée, l'application utilise les paramètres de serveur proxy spécifiés pour se connecter aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites avec le module Protection contre les menaces Internet.
Adresse et port	Champs de saisie de l'adresse IP ou du nom de domaine et du port du serveur proxy. Port par défaut : 3128. Les champs sont accessibles si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée.
Utiliser l'authentification sur le serveur proxy	Cette case active ou désactive l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe pour l'accès au serveur proxy. La case est accessible si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée. La case est décochée par défaut. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.
Nom d'utilisateur	Champ de saisie du nom d'utilisateur pour son authentification sur le serveur proxy. Le champ de saisie est disponible si la case **Utiliser l'authentification sur le serveur proxy** est cochée.
Mot de passe	Champ de saisie du mot de passe de l'utilisateur pour l'authentification sur le serveur proxy. Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois. Cliquez sur le bouton **Afficher** pour afficher le mot de passe de l'utilisateur en clair dans le champ **Mot de passe**. Par défaut, le mot de passe de l'utilisateur est masqué et s'affiche sous forme de points. Le champ de saisie et le bouton sont accessibles si la case **Utiliser l'authentification sur le serveur proxy** est cochée.
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation	Active ou désactive l'utilisation du Serveur d'administration de Kaspersky Security Center comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky. Cela est nécessaire lors de l'activation de l'application dans un segment isolé du réseau sans accès à Internet à l'aide d'un code d'activation. Si la case est sélectionnée, l'application accède aux serveurs d'activation via le Serveur d'administration avec accès à Internet. La case est décochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. Si l'application est utilisée en mode Light Agent, les informations sur la licence sont fournies par le Serveur de protection.
Exclusions pour le serveur proxy	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions pour le serveur proxy**.

Fenêtre Exclusions pour le serveur proxy

Dans cette fenêtre, vous pouvez configurer l'utilisation d'un serveur proxy lors de l'intégration avec les modules de la solution Kaspersky Anti Targeted Attack Platform, ainsi qu'une liste d'adresses pour se connecter auxquelles aucun serveur proxy ne sera utilisé.

Exclusions pour le serveur proxy

Paramètre	Description
Ne pas utiliser le serveur proxy lors de l'exécution des modules	Cochez les cases en regard des modules d'application pour lesquels vous ne souhaitez pas utiliser le serveur proxy : • **Endpoint Detection and Response Expert (on-premises)** : ne pas utiliser de serveur proxy lors de la connexion à des serveurs qui assurent l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA). • **Sandbox** : ne pas utiliser de serveur proxy pour vous connecter aux serveurs qui offrent une intégration avec Sandbox. • **Network Detection and Response (KATA)** : ne pas utiliser de serveur proxy lors de la connexion à des serveurs qui offrent une intégration avec Kaspersky Network Detection and Response (KATA).
Ne pas utiliser de serveur proxy pour les adresses	Le tableau contient une liste d'adresses pour lesquelles le serveur proxy ne sera pas utilisé pour se connecter : • **Adresse IP/nom DNS** : adresse IP ou nom DNS pour se connecter auquel aucun serveur proxy ne sera utilisé. Pour spécifier l'adresse, vous pouvez utiliser des masques (symboles `*` et `?`). • **Commentaire** : champ de saisie pour un commentaire (facultatif). Vous pouvez ajouter, modifier ou supprimer des adresses dans le tableau.

Utilisation du processeur par les tâches d'analyse

Dans la Console d'administration, vous pouvez activer ou désactiver la limite d'utilisation du processeur et configurer la limite d'utilisation de la mémoire pour les tâches d'analyse dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, section **Performances**).

Un clic sur **Configurer** sous **Performances** ouvre la fenêtre **Paramètres des performances des tâches d'analyse**, dans laquelle vous pouvez configurer les limites dans la section **Consommation du processeur et de la mémoire** (voir le tableau ci-dessous).

Paramètres d'utilisation du processeur et de la mémoire

Paramètre	Description
Limiter la consommation de ressources du processeur pour les tâches d'analyse (%)	La case active ou désactive la limite d'utilisation des ressources CPU pour les tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse du conteneur*. Si la case est cochée, la charge maximale sur tous les noyaux du processeur lors de l'exécution de ces tâches ne dépasse pas la valeur spécifiée dans le champ de droite (en pourcentage). La valeur dans le champ doit être un entier et être comprise entre 10 et 100. La case est décochée par défaut.
Limite d'utilisation de la mémoire pour les tâches d'analyse (Mo)	Champ de saisie permettant de limiter l'utilisation de la mémoire pour les tâches d'analyse (en mégaoctets). Valeur par défaut : 8192.

Exécution de tâches sur batterie

Dans la Console d'administration, vous pouvez configurer l'annulation des tâches planifiées dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, section **Performances**).

Paramètres des tâches lors de l'utilisation de la batterie

Paramètre	Description
Ignorer les tâches planifiées lors du fonctionnement sur batterie	Cette case à cocher active ou désactive l'annulation des tâches planifiées. La case est cochée par défaut. Si la case est décochée, toutes les tâches planifiées sont exécutées sur l'appareil, quelle que soit la source d'alimentation à laquelle l'appareil est connecté (réseau ou batterie).

Lancement de l'application

Dans la Console d'administration, vous pouvez gérer les paramètres de lancement de l'application dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, section **Paramètres de lancement de l'application**).

Dans le groupe **Paramètres de démarrage de l'application**, cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Paramètres de démarrage de l'application**, dans laquelle vous pouvez configurer les paramètres de lancement de l'application (cf. le tableau ci-dessous).

Paramètres de démarrage de l'application

Paramètre	Description
Nombre maximum de tentatives consécutives infructueuses pour démarrer une application	Champ de saisie du nombre maximum de tentatives consécutives infructueuses de lancement de l'application. Valeur par défaut : 5.
Durée maximale d'attente pour le démarrage de l'application (min)	Champ de saisie du temps maximum d'attente pour le démarrage de l'application (en minutes), après quoi le processus kesl sera redémarré. Valeur par défaut : 3.

Redémarrage automatique à la réception d'une mise à jour critique

Dans la Console d'administration, vous pouvez configurer le redémarrage automatique de l'application lors de l'installation des mises à jour critiques dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**).

Dans la section **Paramètres d'application avancés**, un clic sur le bouton **Configurer** ouvre la fenêtre **Paramètres avancés**, dans laquelle vous pouvez configurer le redémarrage de l'application lors de la réception de mises à jour critiques (cf. le tableau ci-dessous).

Paramètres d'application des mises à jour critiques

Paramètre	Description
Redémarrer automatiquement l'application lors de la réception de mises à jour critiques	Cette case active ou désactive le redémarrage automatique de l'application lorsque des mises à jour critiques sont reçues au-delà des 24 premières heures suivant l'installation de l'application. La case est décochée par défaut. Si cette case est cochée, l'application redémarre après les mises à jour critiques si 24 heures se sont écoulées depuis l'installation.

Protection par mot de passe

Dans la Console d'administration, vous pouvez configurer les paramètres de la Protection par mot de passe dans les propriétés de la stratégie (**Paramètres généraux** → **Interface**, section **Protection par mot de passe**).

Dans la section **Protection par mot de passe**, un clic sur le bouton **Configurer** ouvre la fenêtre **Paramètres de la protection par mot de passe**, dans laquelle vous pouvez modifier les paramètres de la Protection par mot de passe (voir le tableau ci-dessous).

Paramètres de démarrage de l'application

Paramètre	Description
Activer la protection par mot de passe	Cette case active ou désactive la protection par mot de passe des paramètres de l'application. La case est décochée par défaut.
Autorisations	Ce tableau contient les utilisateurs et les groupes pour lesquels vous pouvez configurer les autorisations de modification des paramètres de l'application. Le tableau contient les colonnes suivantes : • **Utilisateur/Groupe** est le nom de l'utilisateur local ou de domaine, ou le nom du groupe d'utilisateurs pour lequel les autorisations sont configurées. • **Type** est soit **Utilisateur**, soit **Groupe** pour lequel des autorisations sont configurées. • **Autorisations** est une liste d'opérations que l'utilisateur ou le groupe est autorisé à effectuer. Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs. Vous pouvez cliquer sur le bouton **Ajouter** pour ouvrir la fenêtre **Autorisations d'un utilisateur/groupe**, dans laquelle vous pouvez ajouter un utilisateur ou un groupe et définir les autorisations de modification des paramètres de l'application.

Paramètres de traçage et d'enregistrement de vidage

Dans la Console d'administration, vous pouvez gérer les paramètres de traçage et d'enregistrement des vidages dans les propriétés de la stratégie (**Paramètres généraux → Paramètres de l'application**, section **Paramètres de traçage et d'enregistrement des vidages**).

Sous **Paramètres de traçage et d'enregistrement des vidages**, un clic sur **Configurer** ouvre la fenêtre **Paramètres de traçage et d'enregistrement des vidages** dans laquelle vous pouvez modifier les paramètres de traçage et de vidage (cf. le tableau ci-dessous).

Paramètres de traçage et d'enregistrement de vidage

Paramètre	Description
Chemin d'accès au répertoire contenant les fichiers de traçage	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de traçage sont stockés. Valeur par défaut : /var/log/kaspersky/kesl. Si vous indiquez un autre répertoire, assurez-vous que l'utilisateur qui exécute Kaspersky Endpoint Security dispose des autorisations de lecture et d'écriture pour ce répertoire. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root.
Taille maximale du fichier de traçage (Mo)	Dans ce champ, vous pouvez saisir la taille maximale d'un fichier de traçage d'application (en mégaoctets). Valeur par défaut : 500.
Nombre maximum de fichiers de traçage	Dans ce champ, vous pouvez saisir le nombre maximal de fichiers de traçage d'application. Valeur par défaut : 10.
Créer un fichier des vidages en cas de plantage de l'application	La case active ou désactive la création d'un fichier de vidage lorsque l'application plante. La case est décochée par défaut.
Chemin d'accès au répertoire contenant les fichiers de vidage	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de vidage sont stockés. La taille du champ de saisie est limitée à 128 caractères. Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps.

Utilisation de la mémoire résidente par l'application

Dans la Console d'administration, vous pouvez configurer la limite d'utilisation de la mémoire résidente dans les propriétés de la stratégie (**Paramètres généraux → Paramètres de l'application**).

Dans le groupe **Paramètres d'application avancés**, cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Paramètres avancés**, dans laquelle vous pouvez configurer la limite d'utilisation de la mémoire résidente (cf. le tableau ci-dessous).

Pour appliquer les modifications, redémarrez l'application Kaspersky Endpoint Security sur l'appareil administré après l'application de la stratégie.

Paramètres d'utilisation de la mémoire résidente par l'application

Paramètre	Description
Utilisation de la mémoire par l'application	Dans la liste déroulante, vous pouvez sélectionner comment limiter l'utilisation de la mémoire résidente : • **Pas limitée**. Si cette option est sélectionnée, l'utilisation de la mémoire résidente n'est pas limitée. • **Limitée automatiquement (recommandé)**. Lorsque vous sélectionnez cet élément de la liste, l'utilisation de la mémoire résidente est automatiquement limitée (par défaut). • **Limitée à un pourcentage du volume total**. Lorsque vous sélectionnez cet élément de la liste, le champ **Limite d'utilisation de la mémoire (%)** devient disponible, dans lequel vous pouvez spécifier la valeur de pourcentage souhaitée. • **Limitée à une valeur en mégaoctets**. Lorsque vous sélectionnez cet élément de la liste, le champ **Limite d'utilisation de la mémoire (Mo)** devient disponible, dans lequel vous pouvez spécifier la valeur souhaitée en mégaoctets. • **Limité à la plus petite des valeurs spécifiées (%, Mo)**. Lorsque vous sélectionnez cet élément de la liste, les champs **Limite d'utilisation de la mémoire (%)** et **Limite d'utilisation de la mémoire (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs souhaitées. • **Limité à la plus grande des valeurs spécifiées (%, Mo)**. Lorsque vous sélectionnez cet élément de la liste, les champs **Limite d'utilisation de la mémoire (%)** et **Limite d'utilisation de la mémoire (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs souhaitées.
Limite d'utilisation de la mémoire (%)	Champ de saisie pour limiter l'utilisation de la mémoire (en pourcentage). Valeur par défaut : 50.
Limite d'utilisation de la mémoire (Mo)	Champ de saisie des limites d'utilisation de la mémoire (en mégaoctets). Valeur par défaut : 2000.

Analyse des connexions chiffrées

Dans la Console d'administration, vous pouvez gérer les paramètres d'analyse du trafic réseau dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres réseau**).

Paramètre	Description
Activer l'analyse des connexions chiffrées.	Cette case active ou désactive l'analyse des connexions chiffrées. La case est cochée par défaut.

Paramètres des connexions chiffrées	Le groupe contient les paramètres d'analyse des connexions chiffrées :
	• **Accéder à un domaine dont le certificat n'est pas fiable** : l'action que l'application effectuera lors du passage à un domaine avec un certificat non approuvé :
	  • **Autoriser** (valeur par défaut) : autoriser la connexion à un domaine avec un certificat douteux.
	  • **Bloquer** : bloquer la connexion à un domaine avec un certificat douteux.
	• **Accès à un domaine avec une erreur lors de l'analyse du trafic réseau** : l'action que l'application effectuera lors du passage à un domaine avec une erreur d'analyse du trafic réseau :
	  • **Autoriser et ajouter un domaine aux exclusions** (valeur par défaut) : ajouter le domaine qui a généré l'erreur à la liste des domaines comportant des erreurs d'analyse et ne pas surveiller le trafic réseau chiffré lors de la visite de ce domaine.
	  • **Bloquer** : bloquer la connexion à un domaine avec une erreur d'analyse.
	• **Stratégie de vérification du certificat** : la manière dont l'application valide les certificats :
	  • **Vérification locale** : l'application n'utilise pas Internet pour vérifier un certificat.
	  • **Vérification complète** (valeur par défaut) : l'application utilise Internet pour vérifier et télécharger les chaînes manquantes qui sont nécessaires pour vérifier un certificat.

Domaines de confiance	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Domaines de confiance** dans laquelle vous pouvez configurer une liste de noms de domaine de confiance.
Certificats racines de confiance	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce lien pour ouvrir la fenêtre **Certificats racine de confiance**. Dans cette fenêtre, vous pouvez configurer une liste de certificats racine que Kaspersky Endpoint Security considérera comme fiables lors de l'analyse des connexions chiffrées.
Exclusions de l'interception du trafic	Le groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions de l'interception du trafic**. Dans cette fenêtre, vous pouvez configurer les paramètres des connexions dont l'application exclut le trafic de l'interception.
Paramètres des ports réseau	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Ports contrôlés**.
Paramètres avancés	Le groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Mode d'interception du trafic**. Dans cette fenêtre, vous pouvez configurer le mode d'interception du trafic utilisé par l'application : • **Utiliser la technologie eBPF**. si cette option est sélectionnée, l'application utilise la technologie eBPF pour intercepter le trafic. • **Utiliser l'utilitaire iptables** (valeur par défaut). Si cette option est sélectionnée, l'application utilise l'utilitaire iptables pour intercepter le trafic. Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.

Fenêtre Domaines de confiance

Cette liste contient les noms de domaine et les masques de nom de domaine qui seront exclus de l'analyse. L'application n'analyse pas les connexions établies lors de la visite de domaines spécifiés.

Exemple : `*example.com`. Par exemple, `*example.com/*` n'est pas une valeur valide car elle nécessite une adresse de domaine et non une page Internet.

Par défaut, la liste est vide. Vous pouvez ajouter, modifier et supprimer des domaines dans la liste des domaines de confiance.

Fenêtre Certificats de confiance

Vous pouvez configurer la liste des certificats racines que l'application Kaspersky Endpoint Security considérera comme fiables. La liste des certificats racine de confiance est utilisée lors de l'analyse des connexions chiffrées.

Les informations suivantes sont affichées pour chaque certificat :

- Objet du certificat
- Numéro de série du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- empreinte digitale du certificat SHA256.

Par défaut, la liste des certificats est vide.

Vous pouvez ajouter et supprimer des certificats.

Cliquer sur le bouton **Ajouter** ouvre une fenêtre permettant d'ajouter un certificat à la liste des certificats de confiance de l'une des manières suivantes :

- Spécifier le chemin d'accès au fichier de certificat. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Spécifiez le chemin d'accès au fichier au format DER ou PEM contenant le certificat.
- Copiez le contenu du fichier de certificat dans le champ **Saisir les détails du certificat**.

Fenêtre Exclusions de l'interception du trafic

Le tableau contient les paramètres de connexion que l'application exclut de l'interception du trafic :

- **Adresse IP à distance** : l'adresse IP vers laquelle ou depuis laquelle le trafic est exclu de l'interception (selon la direction du trafic).
- **Port de destination** : un port sur un appareil protégé (exclu de l'interception du trafic entrant) ou un port sur un appareil à distance (exclu de l'interception du trafic sortant).
- **Direction du trafic** : la direction du trafic dans la connexion : entrant ou sortant.

Vous pouvez ajouter, modifier et supprimer des exclusions.

Fenêtre Exclusion de l'interception du trafic

Dans cette fenêtre, vous pouvez ajouter une exclusion à l'interception du trafic. Pour ce faire, vous devez spécifier les paramètres de connexion suivants :

- **Adresse IP à distance** : l'adresse de l'appareil à distance au format IPv4 ou IPv6. Selon le sens du trafic, le trafic provenant de l'adresse IP spécifiée (exclusion du trafic entrant) ou le trafic vers l'adresse IP spécifiée (exclusion de trafic sortant) sera exclu.
- **Port de destination** : selon la direction de circulation :
  - Port sur l'appareil protégé (sauf pour le trafic entrant). Le trafic vers ce port provenant des appareils à distance sera exclu de l'interception.
  - Port sur l'appareil à distance (sauf pour le trafic sortant). Le trafic vers ce port provenant de l'appareil protégé sera exclu de l'interception.
- **Direction du trafic** : la direction du trafic dans la connexion exclue. Vous pouvez configurer une exclusion pour le trafic entrant ou pour le trafic sortant.

Vous pouvez spécifier uniquement l'adresse IP de l'appareil à distance ou uniquement le port de destination dans l'exclusion.

Si vous spécifiez uniquement l'adresse IP de l'appareil à distance (sans spécifier le port sur l'appareil protégé) dans l'exclusion pour le trafic entrant, tout le trafic provenant de l'appareil à distance est exclu de l'interception. Il est recommandé de configurer une telle exclusion uniquement pour le trafic provenant d'appareils auxquels vous faites confiance.

Fenêtre Ports contrôlés

Paramètres des ports réseau

Paramètre	Description
Surveiller tous les ports réseau	Si cette option est sélectionnée, l'application surveille tous les ports réseau.
Contrôler uniquement les ports réseau sélectionnés	Si cette option est sélectionnée, l'application surveille uniquement les ports réseau renseignés dans le tableau. Cette option est sélectionnée par défaut.
Paramètres des ports réseau	Le tableau contient les ports réseaux que l'application contrôlera quand l'option **Contrôler uniquement les ports indiqués** est sélectionnée. Le tableau contient deux colonnes : • **Port** : le port contrôlé. • **Description** : description du port contrôlé. Par défaut, le tableau affiche une liste des ports réseau normalement utilisés pour la transmission des emails et du trafic réseau. Cette liste de ports réseau est incluse dans le paquet de l'application. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Exclusions globales

Dans la Console d'administration, vous pouvez configurer des exclusions globales dans les propriétés de la stratégie (**Paramètres généraux** → **Exclusions globales**).

Le groupe de paramètres **Points de montage exclus** contient un bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Points de montage exclus**.

La liste dans la fenêtre contient les chemins vers les points de montage exclus. Par défaut, la liste est vide.

Vous pouvez ajouter, modifier et supprimer des éléments dans la liste.

Fenêtre Chemin du point de montage

Paramètres de point de montage

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres vous permet de spécifier l'emplacement du point de montage. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'analyse : • **Local** : points de montage locaux. • **Monté** : répertoires distants montés sur l'appareil via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : tous les ressources de système de fichiers de l'appareil indiqué dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au point de montage que vous souhaitez ajouter aux exclusions de l'interception des opérations de fichier. Vous pouvez utiliser des masques pour spécifier le chemin. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'interception des opérations de fichier. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Exclure la mémoire de processus de l'analyse

Dans la Console d'administration, vous pouvez configurer l'exclusion de la mémoire des processus de l'analyse dans les propriétés de la stratégie (**Paramètres généraux** → **Exclure la mémoire des processus**).

Cliquer sur le bouton **Configurer** dans le groupe **Exclure la mémoire de processus de l'analyse** ouvre une fenêtre dans laquelle vous pouvez créer une liste d'exclusions.

La liste de la fenêtre **Exclure la mémoire de processus de l'analyse** contient les chemins d'accès aux processus que l'application exclut de l'analyse de la mémoire de processus. Vous pouvez utiliser des masques pour spécifier le chemin. Par défaut, la liste est vide.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cocher la case **Fusionner les valeurs lors de l'héritage** dans la fenêtre **Exclure la mémoire du processus de l'analyse**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Articles utiles

Comment spécifier des masques

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Sauvegarde

Dans la Console d'administration, vous pouvez gérer les paramètres de la Sauvegarde dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres des stockages**) et dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres des stockages**).

Paramètres de sauvegarde

Paramètre	Description
Ne pas conserver les objets plus de (jours)	La case active ou désactive la limitation de la période de stockage des objets dans la sauvegarde selon un intervalle de temps spécifié. Valeurs admises : 0 à 10000. Si la valeur définie est 0, les objets sont conservés dans la sauvegarde pour une période indéterminée. Valeur par défaut : 30.
Limiter la taille de la sauvegarde à (Mo)	La case active ou désactive la limitation de la taille maximale de la sauvegarde par la valeur spécifiée (en mégaoctets). Valeurs admises : 1 à 4000. Si la case est décochée, la taille de la sauvegarde n'est pas limitée. La case est décochée par défaut.

Détection des applications que les intrus peuvent utiliser pour causer des dommages

Dans la Console d'administration, vous pouvez configurer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données dans les propriétés de la stratégie (**Paramètres généraux → Paramètres de l'application**, section **Paramètres d'analyse**).

Paramètres de détection des applications que les intrus peuvent utiliser pour endommager les appareils ou les données

Paramètre	Description
Détecter les applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données	Cette case active ou désactive la détection des applications légitimes qui pourraient être utilisées par des individus malintentionnés pour nuire aux ordinateurs ou aux données des utilisateurs. La case est décochée par défaut.

Interception des opérations sur les fichiers

Dans la Console d'administration, vous pouvez configurer le mode d'interception des opérations sur les fichiers dans les propriétés de la stratégie (**Paramètres généraux → Paramètres de l'application**, section **Mode d'interception des opérations sur les fichiers**).

Paramètres d'interception des opérations sur les fichiers

Paramètre	Description
Bloquer l'accès aux fichiers pendant l'analyse	Cette case à cocher active ou désactive le blocage de l'accès aux fichiers pendant qu'ils sont analysés par les modules Protection contre les fichiers malicieux et Contrôle des appareils, l'action Prévention de l'exécution et la tâche Analyse des disques amovibles. La case est cochée par défaut. Si la case est décochée, l'accès à n'importe quel fichier est autorisé pendant la durée de l'analyse, et l'analyse s'exécute en mode asynchrone.

Envoi d'informations vers le stockage de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez activer ou désactiver l'envoi d'informations sur les fichiers de la sauvegarde, les fichiers en quarantaine, les fichiers non traités et les appareils connectés au stockage de Kaspersky Security Center.

La liste générale des fichiers mis en quarantaine par les applications de Kaspersky sur les appareils clients est conservée dans Kaspersky Security Center et est également disponible dans la Console d'administration (**Avancés** → **Stockages** → **Quarantaine**).

Une liste générale des fichiers placés dans la sauvegarde par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans la Console d'administration (**Avancés** → **Stockages** → **Sauvegarde**).

Les informations sur les fichiers non traités s'affichent dans la liste des menaces actives de la Console d'administration (**Avancés** → **Stockages** → **Menaces actives**).

Les informations sur les appareils installés sur l'appareil client ou connectés à celui-ci s'affichent dans la liste du matériel de la Console d'administration (**Avancés** → **Stockages** → **Matériel**). Les informations sont transmises si le module Contrôle des appareils est activé.

Les informations sur les applications détectées sur l'appareil client s'affichent également dans la liste des applications de la Console d'administration (**Avancés** → **Gestion des applications** → **Registre des applications**). Les informations sont transmises si le module Contrôle des applications est activé.

Activation et désactivation du transfert de données dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver le transfert de données vers le Serveur d'administration dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres des stockages**, **Transfert de données sur le Serveur d'administration**) ou dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres des stockages**, section **Transfert de données sur le Serveur d'administration**).

En cliquant sur le bouton **Configurer** dans le groupe **Transfert de données vers le Serveur d'administration** , la fenêtre **Paramètres de transfert des données** s'ouvre, dans laquelle vous pouvez activer ou désactiver l'envoi d'informations au Serveur d'administration.

Paramètres de transfert de données vers le Serveur d'administration

Paramètre	Description
À propos des fichiers de quarantaine.	La case à cocher active ou désactive le transfert des informations sur les fichiers mis en quarantaine vers le Serveur d'administration. La case est cochée par défaut.
À propos des fichiers de la sauvegarde.	La case à cocher active ou désactive le transfert des informations sur les fichiers de la sauvegarde vers le Serveur d'administration. La case est cochée par défaut.
À propos des fichiers non traités	La case active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration. La case est cochée par défaut.
À propos des appareils installés	La case active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci. La case est cochée par défaut.
À propos des applications détectées sur l'appareil	La case active ou désactive la transmission au Serveur d'administration de la liste des applications détectées sur l'appareil client à la suite de la tâche d'inventaire. La case est cochée par défaut.

Interception des événements système

Dans la Console d'administration, vous pouvez configurer l'interception des événements système dans les propriétés de la stratégie (**Paramètres généraux → Paramètres d'interaction avec le système d'exploitation**, section **Paramètres d'interception des événements système**).

Ces paramètres ne s'appliquent qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Paramètres d'interception des événements système

Paramètre	Description
Mécanisme d'interception	Le mécanisme d'interception des événements système utilisé par l'application dans son travail : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, l'application utilise le module de noyau mis à jour pour l'interception des événements système.
Si le module de noyau mis à jour ne parvient pas à démarrer	Action effectuée par l'application si le module de noyau mis à jour ne parvient pas à démarrer : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné.

Paramètres avancés de collecte de télémétrie

Dans la Console d'administration, vous pouvez gérer des paramètres supplémentaires de télémétrie dans les propriétés de la stratégie (**Paramètres généraux → Paramètres d'interaction avec le système d'exploitation**, section **Paramètres supplémentaires de télémétrie**).

Paramètres avancés de collecte de télémétrie

Paramètre	Description
Source de la télémétrie	Source de collecte de télémétrie utilisée par Kaspersky Endpoint Security : • **Utiliser eBPF uniquement** : utiliser la technologie eBPF seule pour la collecte de télémétrie. • **Utiliser eBPF et auditd** (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie.
Utilisation d'auditd	Mode d'utilisation du service auditd : • **Mode exclusif** (valeur par défaut) : l'application Kaspersky Endpoint Security utilise le service auditd en mode exclusif. • **Mode multidiffusion** : le service auditd est utilisé en mode multidiffusion. Ce paramètre s'applique uniquement si l'option **Utiliser eBPF et auditd** est sélectionnée pour le paramètre **Source de télémétrie**.

Mode Light Agent

Dans la Console d'administration, vous pouvez gérer les paramètres de connexion du Light Agent aux SVM dans les propriétés de la stratégie (**Mode Light Agent**).

Connexion au serveur d'intégration

Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Une connexion au Serveur d'intégration est requise si vous souhaitez que les Light Agents reçoivent des informations sur la SVM via le Serveur d'intégration, ou si vous souhaitez sécuriser la connexion entre le Serveur de sécurité et le Light Agent.

Cette fenêtre affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. En cliquant sur le bouton **Modifier**, la fenêtre **Connexion au serveur d'intégration** s'ouvre, dans laquelle vous pouvez configurer la connexion au Serveur d'intégration.

Fenêtre Connexion au serveur d'intégration

Dans cette fenêtre, vous pouvez spécifier ou modifier les paramètres de connexion des Light Agents au Serveur d'intégration.

Paramètres de connexion au Serveur d'intégration

Paramètre	Description
Adresse	L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center fait partie d'un domaine, le champ par défaut indique le nom de domaine de cet appareil. Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center ne fait pas partie d'un domaine ou si le Serveur d'intégration est installé sur un autre appareil, le champ doit être rempli manuellement. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.
Port	Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Fenêtre Vérification du certificat du Serveur d'intégration

Cette fenêtre s'affiche si le certificat SSL reçu du Serveur d'intégration contient une erreur ou n'est pas approuvé.

À l'aide du lien dans la fenêtre, vous pouvez afficher des informations sur le certificat reçu.

Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

Pour continuer à vous connecter au Serveur d'intégration, cliquez sur le bouton **Ignorer**. Le certificat reçu sera installé en tant que certificat de confiance sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

Fenêtre Authentification sur le Serveur d'intégration

Cette fenêtre s'affiche si l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée ne fait pas partie d'un domaine ou si votre compte n'est pas membre du groupe KLAdmins local ou du domaine ou du groupe des administrateurs locaux.

Spécifiez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **OK**.

Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois.

Après la connexion au Serveur d'intégration avec des droits d'administrateur, la stratégie reçoit automatiquement le mot de passe de l'`agent` utilisé pour connecter les Light Agents au Serveur d'intégration.

Paramètres de détection des SVM

Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Dans cette fenêtre, vous pouvez sélectionner le mode utilisé par les Light Agents pour détecter les SVM disponibles pour la connexion.mode

Paramètres de détection des SVM

Paramètre	Description
Utiliser le Serveur d'intégration	Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant. Si vous souhaitez utiliser le Serveur d'intégration, vous devez configurer les paramètres de connexion des Light Agents au Serveur d'intégration.
Utiliser la liste d'adresses des SVM définie manuellement	Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

Paramètre	Description
Liste des SVM	Une liste d'adresses IP au format IPv4 ou de noms de domaine complets (FQDN) de la SVM auxquels les Light Agents sous contrôle de stratégie peuvent se connecter. En cliquant sur le bouton **Ajouter**, une fenêtre s'ouvre dans laquelle vous pouvez spécifier l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne. Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application. Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**. La liste des adresses SVM s'affiche si l'option **Utiliser la liste d'adresses des SVM définie manuellement** est sélectionnée.

Si vous avez sélectionné l'option **Utiliser la liste d'adresses des SVM définie manuellement** et pour Light Agent, un algorithme de sélection des SVM étendu est utilisé et le mode de protection SVM pour les grandes infrastructures est activé (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez spécifier la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

Tag de connexion à la SVM

Dans cette fenêtre, vous pouvez permettre au Light Agent d'utiliser des tags et attribuer un tag que le Light Agent utilisera pour se connecter.

Assurez-vous que l'utilisation des tags pour les connexions est également configurée dans les paramètres du Serveur de protection : pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent. Les Light Agents dotés d'un tag ne peuvent se connecter qu'aux SVM autorisées à se connecter aux Light Agents avec ce tag.

Paramètres d'utilisation des tags pour la connexion

Paramètre	Description
Utiliser le tag de connexion	La case active ou désactive l'utilisation des tags par le Light Agent pour se connecter à SVM.
Tag	Un tag attribué aux Light Agents. En guise de tag, vous pouvez saisir un texte de 255 caractères maximum. Vous pouvez utiliser n'importe quel caractère à l'exception du caractère `;`. Le champ est disponible si la case **Utiliser le tag de connexion** est cochée.

Algorithme de sélection des SVM

Dans cette fenêtre, vous pouvez spécifier quel algorithme de sélection des SVM les Light Agents doivent utiliser et configurer les paramètres d'utilisation de l'algorithme de sélection des SVM avancé.

Paramètre	Description
Utiliser l'algorithme standard de sélection des SVM	Si cette option est sélectionnée, après l'installation et l'exécution sur une machine virtuelle, Light Agent choisit de se connecter à une SVM locale sur Light Agent. Pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent. Si aucune SVM locale adaptée à la connexion n'est trouvée, le Light Agent sélectionne une SVM à laquelle est connecté le plus petit nombre de Light Agents, quelle que soit la position de la SVM dans l'infrastructure virtuelle. Cette option est sélectionnée par défaut.
Utiliser l'algorithme étendu de sélection des SVM	Si cette option est sélectionnée, vous pouvez utiliser le curseur **Emplacement des SVM** pour spécifier comment l'emplacement de la SVM dans l'infrastructure virtuelle sera pris en compte lors de la détermination de la localité de la SVM par rapport au Light Agent. Le Light Agent ne pourra se connecter qu'aux SVM locales. Vous pouvez également spécifier que l'emplacement de la SVM dans l'infrastructure virtuelle ne doit pas être pris en compte lors de la sélection d'une SVM à laquelle se connecter. Lors de la sélection d'une SVM, les Light Agents prennent en compte le nombre de Light Agents connectés à cette SVM pour garantir une répartition uniforme des Light Agents parmi les SVM disponibles auxquelles se connecter.

Paramètre	Description

Emplacement des SVM	Permet de préciser le type d'emplacement de la SVM dans l'infrastructure virtuelle, qui est pris en compte lors du choix d'une SVM à laquelle se connecter :
	• **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :
	  • La SVM est déployée sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plateforme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
	  • La SVM se trouve dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).
	  • La SVM se trouve sur le même nœud que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).
	  S'il n'y a aucune SVM disponible pour la connexion sur le même hyperviseur ou dans le même groupe de serveurs où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.
	• **Cluster**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :
	  • La SVM est déployée dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plateforme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
	  • Les SVM sont déployées dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle exécutée sur la plateforme OpenStack ou VK Private Cloud).
	  • La SVM se trouve dans la même zone que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Bais Dynamix Enterprise).
	  S'il n'y a aucune SVM disponible à laquelle se connecter dans le même cluster d'hyperviseur ou dans le même projet OpenStack où se trouve la machine virtuelle Light Agent, le Light Agent ne se connecte pas à la SVM.
	• **Centre de données**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :
	  • La SVM est déployée dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plateforme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
	  • La SVM se trouve dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle exécutée sur la plateforme OpenStack ou VK Private Cloud).
	  • La SVM se trouve dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).
	  En l'absence de SVM disponible pour la connexion dans le même centre de données ou la même zone de disponibilité que la machine virtuelle avec le Light Agent, ce dernier ne se connecte pas à la SVM.
	• **Ignorer**. Le Light Agent ne prend pas en compte son emplacement lors du choix d'un SVM.
	Par défaut, la valeur **Hyperviseur** est sélectionnée.
	Le paramètre est disponible si l'option **Utiliser l'algorithme étendu de sélection des SVM** est sélectionnée.

Si un algorithme avancé de sélection de SVM est utilisé pour Light Agent et que la liste des adresses SVM est sélectionnée comme mode de détection de SVM et que le mode de protection pour les grandes infrastructures est activé sur la SVM (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Vous devez définir la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

Protection de la connexion

Dans cette fenêtre, vous pouvez activer le chiffrement du canal de transmission des données entre le Light Agent et le Serveur de protection.

Assurez-vous que le chiffrement du canal de transmission de données entre le Light Agent et le Serveur de protection est activé dans les paramètres du Serveur de protection sur la SVM. Pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent.

Paramètres de sécurité de connexion

Paramètre	Description
Chiffrer le canal de données entre Light Agent et le Serveur de protection	Sécurisez la connexion entre les Light Agents et le Serveur de protection à l'aide du chiffrement. Si la case est cochée, une connexion chiffrée est établie entre le Light Agent, qui est sous contrôle de stratégie, et le Serveur de protection sur la SVM à laquelle le Light Agent se connecte. Un Light Agent dont la protection de connexion est activée peut uniquement se connecter à une SVM sur laquelle la protection de connexion est également activée ou qui autorise une connexion non chiffrée au Serveur de protection. Si la case est décochée, une connexion non chiffrée est établie entre le Light Agent et le Serveur de protection sur la SVM à laquelle le Light Agent se connecte. La case est décochée par défaut.

Problèmes connus et limitations

Limitations de l'application

Kaspersky Endpoint Security n'est pas pris en charge dans les cas suivants :

- Sur les systèmes d'exploitation OSnova en mode d'environnement logiciel fermé et en mode de noyau renforcé.
- Sur les systèmes d'exploitation basés sur Red Hat Enterprise Linux, avec le sous-système IMA.
- Sur les systèmes d'exploitation basés sur Red Hat Enterprise Linux, en mode FIPS.
- Sur les systèmes d'exploitation Ubuntu et les systèmes d'exploitation basés sur SUSE Linux Enterprise Server, avec le système de contrôle d'accès obligatoire AppArmor.
- Avec les systèmes de sécurité Grsecurity (sur tous les systèmes d'exploitation).
- Lorsque le mécanisme seccomp est utilisé (sur tous les systèmes d'exploitation).
- Lorsque les technologies WSL1 et WSL2 sont utilisées (sur tous les systèmes d'exploitation).
- Lorsque certaines options de montage du système de fichiers sont utilisées (par exemple, noexec, nosuid).
- Lorsque Kaspersky Endpoint Security est installé dans un conteneur.

Les solutions Detection and Response peuvent ne pas fonctionner correctement sur les machines virtuelles créées à partir d'une image sur laquelle Kaspersky Endpoint Security for Linux est installé. Lors de l'intégration aux solutions Detection and Response, un identifiant unique (Sensor ID) de l'ordinateur est utilisé. L'application génère cet identifiant lors de l'installation initiale, et il est conservé même après la désinstallation de l'application. Lors du clonage d'une image, la machine virtuelle hérite du Sensor ID, ce qui peut conduire les solutions Detection and Response à identifier plusieurs machines virtuelles comme étant le même appareil.

Limitations de l'application sur certaines architectures

L'application présente des limitations lorsqu'elle est exécutée sur les architectures de processeur suivantes :

Elbrus

- Mode Light Agent : non pris en charge.
- Mode agent EDR : non pris en charge.
- Protection BadUSB : ne fonctionne pas.
- Protection contre les Exploits : ne fonctionne pas.
- Protection contre les menaces Internet : l'analyse heuristique n'est pas disponible lors de l'analyse des pages Internet à la recherche de liens de phishing.

- Intégration de Kaspersky Endpoint Detection and Response Optimum : ne fonctionne pas.
- Intégration de Kaspersky Endpoint Detection and Response Expert (cloud) : ne fonctionne pas.
- Intégration de Kaspersky Endpoint Detection and Response (KATA) : ne fonctionne pas.
- Intégration de Kaspersky Managed Detection and Response : ne fonctionne pas.
- Sandbox : ne fonctionne pas.
- Intégration KUMA : ne fonctionne pas.
- Analyse du conteneur : ne fonctionne pas.
- Module de noyau mis à jour : non pris en charge.
- Interface graphique d'administration : les utilisateurs ne peuvent pas envoyer de fichiers pour analyse dans Sandbox, car le module Sandbox n'est pas pris en charge.

Limitations de l'application sur certains systèmes d'exploitation

L'application présente des limitations lorsqu'elle est exécutée sur les systèmes d'exploitation suivants :

Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)

- Protection BadUSB : ne fonctionne pas, car le service systemd-logind est absent du système d'exploitation.
- La limitation de l'utilisation des ressources du processeur pour les tâches Analyse des logiciels malveillants, Analyse des zones critiques, Inventaire et Analyse du conteneur ne fonctionne pas sur les noyaux « 4.2.0-23-generic ».

CentOS 5.2 et 5.4

- Détection comportementale : le bon fonctionnement du module n'est pas garanti, car l'interception synchrone des démarrages de processus n'est pas disponible.
- Protection contre les menaces par emails : ne fonctionne pas.
- Protection contre les menaces Internet : ne fonctionne pas, car le mécanisme TProxy n'est pas pris en charge.
- Protection contre les menaces réseau : ne fonctionne pas, car le mécanisme TProxy n'est pas pris en charge.
- Protection contre le chiffrement : ne fonctionne pas, car le mécanisme TProxy n'est pas pris en charge.
- Protection BadUSB : ne fonctionne pas, car le service systemd-logind est absent du système d'exploitation.
- Analyse du conteneur : ne fonctionne pas, car le système d'exploitation ne prend pas en charge les conteneurs.
- Contrôle des appareils : le mode Lecture seule des appareils ne fonctionne que si l'appareil a été connecté après l'activation du mode dans l'application. Pour les appareils connectés avant l'activation de ce mode, le mode d'accès reste inchangé.

- Contrôle des applications : ne fonctionne pas, car la technologie fanotify nécessaire à l'interception synchrone du démarrage des processus n'est pas prise en charge.
- Gestion du pare-feu : ne fonctionne pas, car l'ajout de chaînes à iptables n'est pas pris en charge.
- Contrôle Internet : ne fonctionne pas, car le mécanisme TProxy n'est pas pris en charge.
- Module de noyau mis à jour : non pris en charge.
- Isolation du réseau : ne fonctionne pas, car le mécanisme TProxy n'est pas pris en charge.
- La prévention de l'exécution pour les objets ne fonctionne pas, car il n'y a pas d'interception synchrone du démarrage des processus.
- Intégration de Kaspersky Endpoint Detection and Response Optimum : ne fonctionne pas.
- Intégration de Kaspersky Endpoint Detection and Response Expert (cloud) : ne fonctionne pas.
- Intégration à Kaspersky Endpoint Detection and Response (KATA) : la source de télémétrie eBPF n'est pas disponible.
- Intégration à Kaspersky Managed Detection and Response : la source de télémétrie auditd n'est pas disponible.
- Interface utilisateur graphique : ne fonctionne pas, car la bibliothèque libxcb est absente du système d'exploitation.
- Agent d'administration de Kaspersky Security Center : nécessite une configuration complémentaire de l'appareil. Consultez l'aide de Kaspersky Security Center.
- Installation/suppression : l'application n'est pas compatible avec SELinux dans cette version du système d'exploitation. Solution possible : faites passer SELinux en mode non bloquant (mode permissif), désactivez SELinux ou configurez manuellement SELinux.
- Analyse des logiciels malveillants : dans les systèmes d'exploitation dotés de versions de glibc antérieures à 2.11, les fichiers situés dans des répertoires dont le chemin d'accès dépasse 4096 caractères ne sont pas désinfectés ni supprimés.
- La limitation de l'utilisation des ressources du processeur pour les tâches Analyse des logiciels malveillants, Analyse des zones critiques, Inventaire et Analyse du conteneur ne fonctionne pas.
- Le mode Light Agent n'est pas pris en charge. Par conséquent, les paramètres KSVLA_MODE, SERVER_MODE et VDI_MODE ne sont pas applicables lors de l'installation de l'application.
- Le fonctionnement de l'application en mode agent EDR n'est pas pris en charge.
- L'application n'est pas prise en charge dans Kaspersky Security Center Cloud Console.
- L'application ne prend pas en charge les systèmes de fichiers basés sur la technologie FUSE.
- Les statistiques des fichiers les plus fréquemment analysés ne sont pas collectées.
- Dans certains cas, la télémétrie transmise dans le cadre de l'intégration à Kaspersky Endpoint Detection and Response (KATA) peut contenir des informations incomplètes sur les événements des journaux d'événements système.

CentOS 6.4 et 6.6

- Détection comportementale : le bon fonctionnement du module n'est pas garanti, car l'interception synchrone des démarrages de processus n'est pas disponible.
- Protection contre les menaces Internet : l'interception du trafic IPv6 ne fonctionne pas.
- Protection contre les menaces réseau : l'interception du trafic IPv6 ne fonctionne pas.
- Protection contre le chiffrement : l'interception du trafic IPv6 ne fonctionne pas.
- Protection BadUSB : ne fonctionne pas, car le service systemd-logind est absent du système d'exploitation.
- Analyse du conteneur : ne fonctionne pas, car le système d'exploitation ne prend pas en charge les conteneurs.
- Contrôle des applications : ne fonctionne pas, car la technologie fanotify nécessaire à l'interception synchrone du démarrage des processus n'est pas prise en charge.
- Gestion du pare-feu : les règles IPv6 du pare-feu ne fonctionnent pas.
- Contrôle Internet : l'interception du trafic IPv6 ne fonctionne pas.
- Module de noyau mis à jour : non pris en charge.
- La prévention de l'exécution pour les objets ne fonctionne pas, car il n'y a pas d'interception synchrone du démarrage des processus.
- Kaspersky Endpoint Detection and Response Optimum : la chaîne de développement de la menace ne représente pas l'activité réseau, car TProxy n'est pas pris en charge. Seuls les événements de télémétrie relatifs aux opérations sur les fichiers sont disponibles. La prévention de l'exécution des objets ne fonctionne pas, car l'interception synchrone du démarrage des processus n'est pas disponible.
- Intégration de Kaspersky Endpoint Detection and Response Expert (cloud) : ne fonctionne pas.
- Intégration à Kaspersky Endpoint Detection and Response (KATA) : la source de télémétrie eBPF n'est pas disponible.
- Intégration à Kaspersky Managed Detection and Response : la source de télémétrie auditd n'est pas disponible.
- Agent d'administration de Kaspersky Security Center : nécessite une configuration complémentaire de l'appareil. Consultez l'aide de Kaspersky Security Center.
- Installation/suppression : l'application n'est pas compatible avec SELinux dans cette version du système d'exploitation. Solution possible : faites passer SELinux en mode non bloquant (mode permissif), désactivez SELinux ou configurez manuellement SELinux.
- Analyse des logiciels malveillants : dans les systèmes d'exploitation dotés de versions de glibc antérieures à 2.11, les fichiers situés dans des répertoires dont le chemin d'accès dépasse 4096 caractères ne sont pas désinfectés ni supprimés.
- Le fonctionnement de l'application en mode Light Agent et en mode agent EDR n'est pas pris en charge.
- L'application n'est pas prise en charge dans Kaspersky Security Center Cloud Console.

- Les statistiques des fichiers les plus fréquemment analysés ne sont pas collectées.
- Dans certains cas, la télémétrie transmise dans le cadre de l'intégration à Kaspersky Endpoint Detection and Response (KATA) peut contenir des informations incomplètes sur les événements des journaux d'événements système.

Limitations liées aux valeurs du paramètre ptrace

Les valeurs du paramètre `kernel.yama.ptrace_scope` du système d'exploitation peuvent affecter Kaspersky Endpoint Security :

- 1 (ptrace limité). Un processus peut se connecter uniquement aux processus qu'il a démarrés. Une autorisation spéciale est requise pour se connecter aux autres processus. Les fonctionnalités de l'application sont limitées comme suit :
  - Le module Détection comportementale ne peut pas obtenir les paramètres d'environnement des processus.
  - Sur les systèmes d'exploitation dotés d'une version de noyau postérieure à 5.7, le module Contrôle des applications ne peut pas lire les arguments de ligne de commande et les variables d'environnement des processus, car la lecture de /proc/<pid>/syscall et de /proc/<pid>/mem est interdite. Sur les systèmes d'exploitation dotés de la version de noyau 5.0, le module Contrôle des applications ne peut pas fonctionner correctement.
  - L'analyse de la mémoire des processus et de la mémoire du noyau ne fonctionne pas dans les tâches d'analyse, car la lecture de /proc/<pid>/mem est interdite.
  - L'analyse YARA de la mémoire des processus n'est pas garantie, car la lecture de /proc/<pid>/mem n'est pas autorisée.
- 2 (ptrace administratif). Seuls les processus dotés des privilèges CAP_SYS_PTRACE (généralement root) peuvent utiliser ptrace ou accéder à un processus dans /proc (/proc/<pid>/mem). Le dépannage est limité dans la mesure où les vidages sur incident ne fonctionnent pas pour les processus utilisateur (tels que kesl-control et kesl-gui), bien que les vidages fonctionnent pour le processus kesl lui-même.
- 3 (ptrace interdit) : ptrace entièrement interdit au niveau du système d'exploitation. Les fonctionnalités de l'application sont limitées comme suit :
  - Les vidages sur incident ne fonctionnent pas pour le processus kesl ni pour les processus utilisateur (tels que kesl-control et kesl-gui).
  - Le module Détection comportementale ne peut pas obtenir les paramètres d'environnement des processus.
  - Le module Contrôle des applications n'est pas pris en charge.

- Comme le répertoire /proc/<pid>/mem ne peut pas être lu :
  - L'analyse de la mémoire des processus et de la mémoire du noyau ne fonctionne pas dans les tâches d'analyse.
  - Les tâches Obtenir le vidage mémoire et Obtenir le vidage mémoire du processus ne fonctionnent pas dans le cadre de l'intégration à des solutions Detection and Response.
  - Les analyses YARA de la mémoire des processus ne sont pas garanties en mode de contrôle d'accès obligatoire lors de l'intégration à Kaspersky Endpoint Detection and Response Expert (on-premises).

Limitations du module de noyau mis à jour

Le module de noyau mis à jour ne prend pas en charge les types et versions de noyaux suivants :

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

RED OS 7.3

- `kernel-ml-5.14.9-1.el7`

RED OS 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

Limitations sur l'utilisation de la technologie eBPF

Pour utiliser la technologie eBPF pour intercepter le trafic réseau, vous avez besoin d'un noyau Linux 4.18 ou version ultérieure, compilé avec les options suivantes :

- `CONFIG_DEBUG_INFO_BTF=y` or `m` (prise en charge d'eBPF avec BTF)
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

Pour utiliser eBPF pour l'envoi de télémétrie lors de l'intégration avec des solutions Detection and Response, vous avez besoin d'un noyau Linux 4.18 ou version ultérieure, compilé avec les options suivantes :

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`

- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

Considérations particulières

- L'application ne peut pas être utilisée simultanément en mode Light Agent et en mode EDR Agent.
- Sur les systèmes d'exploitation dotés d'auditd 3.0.7 et du noyau Linux 4.18, l'utilisation du module Détection comportementale peut entraîner le blocage de l'application et des connexions SSH.
- Sur les systèmes d'exploitation Kylin Desktop V10 SP1 2303, le module Détection comportementale peut bloquer le système d'exploitation. Pour résoudre ce problème, nous vous recommandons de mettre à jour le noyau du système d'exploitation.
- Pour les règles du Contrôle des applications dans Web Console, le paramètre **Refuser pour les autres utilisateurs** s'affiche. Ce paramètre n'est pas utilisé par l'application et n'a aucune incidence sur le fonctionnement des règles du Contrôle des applications.

Considérations particulières pour le mode Light Agent

Si Kaspersky Endpoint Security est utilisé en mode Light Agent :

- L'application ne peut pas être administrée à l'aide de Kaspersky Security Center Cloud Console et de l'interface utilisateur graphique.
- L'utilisation de bases cloud n'est pas prise en charge.
- Kaspersky Endpoint Security interagit avec les serveurs KSN à l'aide du serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge.
- L'utilisation du serveur proxy de l'application n'est pas prise en charge lors de la connexion au Serveur d'intégration, à la SVM et au serveurs KSN.

Considérations particulières pour le mode EDR Agent

Si vous utilisez Kaspersky Endpoint Security en mode EDR Agent, l'ensemble des modules et des tâches disponibles pour l'application est limité. Après l'installation, les paramètres de l'application sont configurés comme suit :

- L'intégration de Kaspersky Endpoint Detection and Response Expert (cloud) n'est pas prise en charge.
- Modules entièrement gérables assurant l'intégration avec les solutions Detection and Response :
  - EDR Expert (on-premises)
  - NDR (KATA).

  Ces modules sont désactivés par défaut ; vous devez les activer pour que l'application fonctionne en mode EDR Agent. Vous pouvez personnaliser les paramètres d'intégration, y compris la fonctionnalité de prévention du lancement des objets.
- L'accès aux fichiers n'est pas bloqué pendant l'analyse : la case **Bloquer l'accès aux fichiers pendant l'analyse** est décochée (`FileBlockDuringScan=No`). Ce paramètre peut être modifié, mais n'est pas appliqué sur l'appareil protégé.
- Les modules Protection contre les fichiers malicieux et Protection contre le chiffrement sont disponibles en mode de fonctionnalités limitées : lorsqu'une menace est détectée, ces modules ne tentent pas de désinfecter ou de supprimer les objets malveillants, de refuser l'accès ou de bloquer l'activité de l'application, mais envoient uniquement des informations sur la détection de la menace à des serveurs qui assurent l'intégration avec les solutions Detection and Response.

  Vous pouvez activer ou désactiver la Protection contre les fichiers malicieux et la Protection contre le chiffrement, et configurer les paramètres des modules, à l'exception des actions lors de la détection d'une menace. Les paramètres suivants ne sont pas appliqués sur l'appareil protégé :
  - Module Protection contre les fichiers malicieux : **Action lors de la détection d'une menace** : **Ignorer** (`ActionOnThreat=Skip`).
  - Module Protection contre le chiffrement : **Action lors de la détection du chiffrement** : **Informer** (`ActionOnDetect=Notify`).
- Le module Détection comportementale est entièrement administrable.
- Tous les autres modules de protection et de contrôle sont désactivés et inaccessibles à l'administration.

Lors de l'intégration à Kaspersky Endpoint Detection and Response Expert (on-premises) ou à Kaspersky Endpoint Detection and Response (KATA), dans le cadre d'une action de réponse aux menaces, Kaspersky Endpoint Security peut contrôler le lancement des fichiers exécutables et des scripts sur l'appareil. La fonctionnalité Prévention du lancement des objets est disponible avec les limitations suivantes :

- Si un script est exécuté depuis l'interpréteur, l'application n'a aucun contrôle sur le lancement du script.
- L'application ne contrôle pas l'ouverture des fichiers des applications Office sur l'appareil.

Contacter le Support technique

Si la solution à votre problème ne figure pas dans la documentation de l'application ou dans une des sources d'informations consacrées à l'application, nous vous conseillons de contacter le Support technique de Kaspersky. Les experts du Support technique répondront à toutes vos questions sur l'installation et l'utilisation de Kaspersky Endpoint Security.

Kaspersky assure la prise en charge de chaque version de Kaspersky Endpoint Security pendant le cycle de vie de cette version (consultez la page du cycle de vie de l'application). Avant de contacter le Support technique, veuillez prendre connaissance des règles d'octroi de l'assistance technique.

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

- visiter le site Internet du Support technique ;
- envoyer une demande au Support technique de Kaspersky via le portail Kaspersky CompanyAccount.

Support technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail à disposition des entreprises qui utilisent les applications de Kaspersky. Kaspersky CompanyAccount permet aux organisations qui utilisent les applications de Kaspersky de contacter le Support technique de Kaspersky au moyen de demandes par e-mail. Sur le portail, vous pouvez créer de nouvelles demandes, suivre leur progression et conserver un historique du traitement des demandes.

Enregistrez tous les employés de votre organisation sous un compte unique sur Kaspersky CompanyAccount. Cela vous permettra de gérer de manière centralisée les demandes électroniques adressées à Kaspersky et de contrôler l'accès de vos utilisateurs à Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Pour en savoir plus sur Kaspersky CompanyAccount, consultez le site Internet du Support technique de Kaspersky CompanyAccount.

Obtention d'informations pour le Support technique

Après que vous avez informé les spécialistes du Support technique de Kaspersky du problème, ceux-ci peuvent vous demander d'envoyer *un fichier de traçage* ou *un fichier de vidage*.

En outre, les spécialistes du Support technique peuvent avoir besoin d'informations supplémentaires sur le système d'exploitation, les processus en cours d'exécution sur l'appareil et des rapports détaillés sur le fonctionnement des modules de l'application.

Lors des diagnostics, les spécialistes du Support technique peuvent vous demander de modifier les paramètres de l'application :

- activer la fonctionnalité d'obtention d'informations de diagnostic étendues ;
- affiner le fonctionnement des modules individuels de l'application, ce qui n'est pas disponible via les outils d'interface utilisateur standard ;
- modifier les paramètres de stockage des informations de diagnostic obtenues ;
- configurer l'interception du trafic réseau et l'enregistrement dans un fichier.

Toutes les informations nécessaires à l'exécution des actions ci-dessus (une description de la séquence des étapes, les paramètres modifiables, les fichiers de configuration, les scripts, les options de ligne de commande supplémentaires, les modules de débogage, les utilitaires spécialisés, etc.), ainsi que la composition des données obtenues à des fins de débogage, vous seront communiquées par les spécialistes du Support technique. Les informations de diagnostic étendues obtenues sont stockées sur l'appareil de l'utilisateur. Les données obtenues ne sont pas automatiquement envoyées à Kaspersky.

Il est conseillé de réaliser les opérations citées ci-dessus en suivant les instructions des spécialistes du Support technique. Si vous décidez de modifier vous-même les fichiers de l'application d'une manière non décrite dans la documentation de l'application ou dans les recommandations des spécialistes du Support technique, ces modifications pourraient entraîner des ralentissements et des pannes dans le fonctionnement de l'application et du système d'exploitation, une diminution du niveau de protection de votre appareil, ainsi qu'une violation de la disponibilité et de l'intégrité des informations traitées.

Comment activer et configurer la création de fichiers de traçage

Le *fichier de traçage* de l'application Kaspersky Endpoint Security vous permet de suivre l'exécution étape par étape des commandes de l'application et de détecter à quelle étape de l'application une erreur se produit.

Par défaut, les fichiers de traçage de l'application ne sont pas générés. Vous pouvez activer ou désactiver la création de fichiers de traçage et sélectionner le niveau de traçage en ligne de commande, dans les paramètres généraux de l'application ou dans l'interface utilisateur graphique.

Si vous gérez l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez configurer les paramètres de traçage de l'application dans les paramètres de la stratégie de Kaspersky Endpoint Security à l'aide de Web Console ou de la Console d'administration.

Comment gérer les paramètres de traçage dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Paramètres généraux → Assistance technique** et consultez la rubrique **Paramètres de traçage**.
5. Si vous souhaitez modifier le répertoire dans lequel les fichiers de traçage de l'application sont enregistrés par défaut, indiquez le répertoire de stockage des fichiers de traçage dans le champ **Chemin d'accès au dossier de traçage**. Valeur par défaut : /var/log/kaspersky/kesl. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).
6. Si nécessaire, indiquez la taille maximale d'un fichier de traçage de l'application (en mégaoctets) dans le champ **Taille maximale du fichier de traçage (Mo)**. Valeur par défaut : 500.
7. Si nécessaire, indiquez le nombre maximal de fichiers de traçage de l'application dans le champ **Nombre maximum de fichiers de traçage**. Valeur par défaut : 10.
8. Enregistrez vos modifications.
9. Redémarrez l'application pour appliquer les paramètres de traçage.

Comment gérer les paramètres de traçage dans la Console d'administration

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.
4. Accédez à la section **Paramètres généraux → Paramètres de l'application**.
5. Dans **Paramètres de traçage et de vidage**, cliquez sur **Configurer**.
6. La fenêtre **Paramètres de traçage et de vidage** s'ouvre.
7. Si vous souhaitez modifier le répertoire dans lequel les fichiers de traçage de l'application sont enregistrés par défaut, indiquez le répertoire de stockage des fichiers de traçage dans le champ **Chemin d'accès au répertoire des fichiers de traçage**. Valeur par défaut : /var/log/kaspersky/kesl. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).
8. Si nécessaire, indiquez la taille maximale d'un fichier de traçage de l'application (en mégaoctets) dans le champ **Taille maximale du fichier de traçage (Mo)**. Valeur par défaut : 500.

9. Si nécessaire, indiquez le nombre maximal de fichiers de traçage que l'application peut créer dans le champ **Nombre maximal de fichiers de traçage**. Valeur par défaut : 10.

10. Cliquez sur **OK** dans la fenêtre **Paramètres de traçage et de vidage**.

11. Cliquez sur le bouton **Appliquer**.

12. Redémarrez l'application pour appliquer les paramètres de traçage.

Comment activer le traçage et gérer les paramètres de traçage en ligne de commande

En ligne de commande, vous pouvez configurer le traçage à l'aide des paramètres `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` et `TraceMaxFileSize` dans les paramètres généraux de l'application. Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Pour créer un fichier de traçage et configurer les paramètres de traçage en ligne de commande :

1. Activez la création d'un fichier de traçage et sélectionnez le niveau de traçage :

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   Où :

   - `Detailed` : crée un fichier de traçage détaillé.
   - `MediumDetailed` : crée un fichier de traçage contenant des messages d'information et d'erreur.
   - `NotDetailed` : crée un fichier de traçage contenant des notifications relatives aux erreurs.

2. Si vous souhaitez modifier le répertoire dans lequel les fichiers de traçage de l'application sont enregistrés par défaut, indiquez le répertoire de stockage des fichiers de traçage :

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   Où `<path to trace files directory>` est le chemin d'accès au répertoire dans lequel les fichiers de traçage sont stockés. Valeur par défaut : /var/log/kaspersky/kesl. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).

3. Si nécessaire, indiquez le nombre maximal de fichiers de traçage :

   ```
   kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
   ```

   Où `<number of application trace files>` est le nombre maximal de fichiers de traçage de l'application. Valeurs possibles : 1 à 10000 Valeur par défaut : 10.

4. Si nécessaire, indiquez la taille maximale d'un fichier de traçage de l'application (en mégaoctets) :

   ```
   kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
   ```

   Où `<size of an application trace file>` est la taille maximale d'un fichier de traçage en mégaoctets. Valeurs possibles : 1 à 1000 Valeur par défaut : 500.

Après avoir modifié les valeurs des paramètres `TraceFolder`, `TraceMaxFileCount`, `TraceMaxFileSize`, vous devez redémarrer l'application.

Pour désactiver la création de fichiers de traçage, exécutez la commande suivante :

```
kesl-control --set-app-settings TraceLevel=None
```

Comment activer le traçage et gérer les paramètres de traçage dans l'interface graphique

La création et la configuration du niveau de détail du fichier de traçage nécessitent des privilèges d'utilisateur avec le rôle Administrateur (admin).

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Support**.

   La fenêtre **Support** s'ouvre.
3. Cliquez sur le lien **Traçage** pour ouvrir la fenêtre **Traçage**.
4. Dans la liste déroulante **Niveau**, sélectionnez le niveau de détail du fichier de traçage :

   - **Diagnostic (300)** – messages d'erreur uniquement.
   - **Informations (700)** – messages d'information et d'erreur.
   - **Débogage (800)** – fichier de traçage détaillé.

   Nous vous recommandons de clarifier le niveau de détail requis auprès des experts du Support technique de Kaspersky. Le paramètre par défaut est **Diagnostic (300)**.
5. Cliquez sur le bouton **Activer** pour démarrer le processus de traçage.
6. Reproduisez la situation dans laquelle vous rencontrez un problème.
7. Cliquez sur le bouton **Désactiver** pour arrêter le processus de traçage.

Les fichiers de traçage créés sont stockés dans le répertoire /var/log/kaspersky/kesl/.

Vous pouvez également activer et configurer la création des fichiers de traçage du serveur Watchdog.

Comment activer le traçage et gérer les paramètres de traçage du serveur Watchdog via la ligne de commande

Sur la ligne de commande, vous pouvez configurer le traçage du serveur Watchdog à l'aide des paramètres `WdTraceLevel` dans les paramètres généraux de l'application. Vous pouvez modifier les valeurs des paramètres à l'aide de commutateurs de ligne de commande ou d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Créer le fichier de traçage du serveur Watchdog et configurer les paramètres de traçage via la ligne de commande

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

Où :

- `Detailed` : crée un fichier de traçage détaillé.
- `MediumDetailed` : crée un fichier de traçage contenant des messages d'information et d'erreur.
- `NotDetailed` : crée un fichier de traçage contenant des notifications relatives aux erreurs.
- `Product` – définissez la valeur égale à celle du paramètre `TraceLevel` dans les paramètres généraux de l'application. Si `TraceLevel=None`, aucun fichier de traçage n'est généré.

Désactiver la création du fichier de traçage du serveur Watchdog et configurer les paramètres de traçage via la ligne de commande

```
kesl-control --set-app-settings WdTraceLevel=None
```

Par défaut, les fichiers de traçage créés sont enregistrés dans le répertoire /var/log/kaspersky/kesl/. Les privilèges root sont requis pour accéder à ce répertoire. Vous pouvez indiquer un autre répertoire de stockage des fichiers de traçage. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).

Les fichiers de traçage de l'interface graphique et de l'utilitaire de ligne de commande kesl-control sont stockés dans le répertoire /var/log/kaspersky/kesl-user. Pour activer la création de ces fichiers de traçage, vous devez définir la variable d'environnement LFS_ENABLE_ALL_COMPONENTS_LOGGING.

Le stockage des fichiers de traçage de l'application nécessite un espace disque supplémentaire au-delà de celui indiqué dans la configuration matérielle minimale requise.

Les fichiers de traçage sont stockés sur l'appareil aussi longtemps que l'application est en cours d'utilisation et sont supprimés définitivement lorsque l'application est supprimée. Les fichiers de traçage ne sont pas automatiquement envoyés à Kaspersky.

Les fichiers de traçage sont stockés sous une forme lisible. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Fichiers de traçage du plug-in d'administration MMC

Si vous utilisez la Console d'administration pour administrer l'application Kaspersky Endpoint Security, les informations sur les événements survenus lors de l'exécution du plug-in d'administration MMC peuvent être enregistrées dans le fichier de trace du plug-in MMC de Kaspersky Endpoint Security sur l'appareil sur lequel se trouve le Serveur d'administration. Le nom du fichier contient le numéro de version de l'application, la date et l'heure de création du fichier ainsi que l'ID du processus (PID). Ce fichier enregistre des informations sur les événements qui se produisent lors du fonctionnement du plug-in MMC, en particulier sur le fonctionnement des stratégies et des tâches.

Par défaut, les fichiers de trace du plug-in MMC ne sont pas créés. Vous pouvez créer un fichier de trace du plug-in MMC à l'aide de clés de registre. Pour des informations détaillées sur la création de fichiers de traçage, vous pouvez contacter le Support technique.

Tous les fichiers de trace du plug-in MMC générés se trouvent dans le dossier spécifié par l'utilisateur lors de la définition des clés de registre.

Fichiers de traçage du plug-in Internet d'administration

Si vous utilisez Web Console pour administrer l'application Kaspersky Endpoint Security, les informations sur les événements qui se produisent lors du fonctionnement du plug-in d'administration Web peuvent être enregistrées dans les fichiers de traçage du plug-in Web.

Les fichiers de traçage du plug-in Internet sont créés automatiquement si la journalisation des activités de Web Console est activée dans l'Assistant d'installation de Web Console (pour plus de détails, consultez l'Aide de Kaspersky Security Center).

Les fichiers de traçage du plug-in Internet sont enregistrés dans le dossier d'installation de Web Console, dans le sous-dossier des journaux.

Contenu des fichiers de traçage de l'application

Les fichiers de traçage contiennent les informations générales suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.
- Module de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (information, avertissement, critique, erreur).
- Description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande.

Les fichiers de traçage peuvent stocker les informations suivantes en plus des données générales :

- États des modules de l'application et de leurs données d'exploitation.
- Données sur les actions des utilisateurs dans l'application.
- Données sur le matériel installé sur l'appareil.
- Données sur tout objet et événement du système d'exploitation, mais également des informations sur l'activité des utilisateurs.
- Données contenues dans les objets du système d'exploitation (par exemple, le contenu des fichiers qui peuvent contenir des données personnelles de l'utilisateur).
- données de trafic réseau (pour exemple, le contenu des champs de saisie sur un site, comme des informations de carte bancaire ou toutes autres données confidentielles) ;
- Données reçues des serveurs de Kaspersky (telles que la version des bases de l'application).
- données reçues des serveurs KATA, des serveurs OSMP, des serveurs NDR et des serveurs qui assurent l'interaction avec Sandbox ;

- données sur les ressources CPU consommées ;
- données sur les ressources RAM consommées ;
- données sur les opérations de lecture et d'écriture de fichiers par les applications ;
- données sur la quantité d'informations mises en cache nécessaires au fonctionnement de l'application.

Contenu des fichiers de traçage des plug-ins d'administration

Les fichiers de traçage des plug-ins d'administration contiennent les données générales suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.
- Module de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (information, avertissement, critique, erreur).
- Description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande.

En plus des données générales, les fichiers de traçage des plug-ins d'administration peuvent contenir les informations suivantes :

- les données personnelles, notamment nom, prénom et patronyme, si ces données font partie du chemin d'accès aux fichiers ;
- le nom du compte de connexion au système d'exploitation, si le nom du compte fait partie du nom du fichier.
- Nom d'utilisateur et mot de passe du serveur proxy Internet.

Activation et configuration de l'enregistrement des vidages

Un *fichier de vidage* contient toutes les informations sur la mémoire de travail des processus de l'application Kaspersky Endpoint Security au moment de la création du fichier de vidage.

Les fichiers de vidage peuvent contenir des données personnelles. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Par défaut, aucun fichier de vidage n'est créé. Vous pouvez activer ou désactiver l'enregistrement des vidages en cas de défaillance de l'application.

Si vous gérez l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez activer ou désactiver l'enregistrement des vidages et le configurer dans les paramètres de la stratégie de Kaspersky Endpoint Security à l'aide de Web Console ou de la Console d'administration.

Si vous utilisez la ligne de commande pour gérer l'application, vous pouvez activer ou désactiver l'enregistrement des vidages via les paramètres généraux de l'application.

Le nombre de fichiers de vidage maximal est limité.

En fonction des paramètres de votre système d'exploitation, les fichiers de vidage personnalisés peuvent ne pas être créés. Assurez-vous que la valeur du paramètre sysctl est `sysctl kernel.yama.ptrace_scope=0`.

Activation et configuration de l'enregistrement des vidages dans Web Console

Pour activer et configurer l'enregistrement des vidages dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Paramètres généraux** → **Assistance technique**, **Informations de débogage**.
5. Si vous souhaitez qu'un fichier de vidage soit généré en cas de plantage de l'application, activez le commutateur **Enregistrement des fichiers dump ACTIVÉ**.
6. Si vous souhaitez modifier le répertoire dans lequel les fichiers de vidage du processus kesl sont enregistrés par défaut, indiquez le répertoire de stockage des fichiers de vidage dans le champ **Chemin d'accès au vidage du code**. Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps. L'accès au répertoire de stockage des fichiers de vidage défini par défaut requiert les autorisations root. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).
7. Enregistrez vos modifications.

Activation et configuration de l'enregistrement des vidages dans la Console d'administration

Pour activer et configurer l'enregistrement des vidages dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.
4. Accédez à la section **Paramètres généraux** → **Paramètres de l'application**.
5. Dans **Paramètres de traçage et de vidage**, cliquez sur **Configurer**.
6. La fenêtre **Paramètres de traçage et de vidage** s'ouvre.
7. Si vous souhaitez qu'un fichier de vidage soit généré en cas de plantage de l'application, cochez la case **Créer un fichier de vidage en cas de plantage de l'application**.

8. Si vous souhaitez modifier le répertoire dans lequel les fichiers de vidage du processus kesl sont enregistrés par défaut, indiquez le répertoire de stockage des fichiers de vidage dans le champ **Chemin d'accès au répertoire du fichier de vidage**. Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps. Des privilèges root sont requis pour accéder au répertoire par défaut des fichiers de vidage (autorisations `700` ou `rwx--------`). Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire.

9. Cliquez sur **OK** dans la fenêtre **Paramètres de traçage et de vidage**.

10. Cliquez sur le bouton **Appliquer**.

Activation et configuration de l'enregistrement des vidages via la ligne de commande

Sur la ligne de commande, vous pouvez activer, désactiver et configurer l'enregistrement des vidages à l'aide des paramètres `CoreDumps` et `CoreDumpsPath` des paramètres généraux de l'application.

Pour activer et configurer l'enregistrement des vidages :

1. Exécutez la commande suivante pour activer l'enregistrement des vidages :

```
kesl --set-app-settings CoreDumps=Yes
```

2. Si vous souhaitez modifier le répertoire dans lequel les fichiers de vidage sont enregistrés, indiquez le chemin d'accès au répertoire dans le paramètre `CoreDumpsPath`.

```
kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
```

Où `<path to directory with dump files>` est le champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de vidage sont stockés. Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps. Des privilèges root sont requis pour accéder au répertoire par défaut des fichiers de vidage (autorisations `700` ou `rwx--------`). Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire.

Pour désactiver l'enregistrement des vidages, exécutez la commande suivante :

```
kesl --set-app-settings CoreDumps=No
```

Si vous avez activé l'enregistrement des vidages, les fichiers de vidage sont stockés par défaut dans les répertoires suivants :

- /var/opt/kaspersky/kesl/common/dumps (fichiers de vidage du processus kesl) ;
- /var/opt/kaspersky/kesl/common/dumps-user (fichiers de vidage du processus utilisateur).

L'accès au répertoire de stockage des fichiers de vidage défini par défaut requiert les autorisations root. Vous pouvez spécifier un autre répertoire pour stocker les fichiers de vidage du processus kesl. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).

Le stockage des fichiers de vidage nécessite un espace disque supplémentaire au-delà de celui spécifié dans la configuration matérielle minimale requise.

Les fichiers dump sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application. Les fichiers de vidage ne sont pas automatiquement envoyés à Kaspersky.

Diagnostic à distance de l'appareil à l'aide de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez effectuer des diagnostics à distance des appareils clients. La procédure de diagnostic à distance permet d'effectuer les opérations suivantes à distance :

- activer et désactiver le traçage ;
- modifier le niveau de traçage ;
- télécharger des fichiers de traçage ;
- télécharger le journal d'installation à distance de l'application ;
- télécharger les journaux d'événements système (syslog) ;
- démarrer, arrêter et redémarrer les applications.

Diagnostics à distance à l'aide de Web Console

Si vous gérez l'application Kaspersky Endpoint Security via Web Console, les diagnostics à distance de l'appareil client sont effectués dans la fenêtre des diagnostics à distance.

Pour ouvrir la fenêtre de diagnostic à distance de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez l'appareil pour lequel vous souhaitez effectuer des diagnostics à distance et cliquez sur le lien <nom de l'appareil>.

   La fenêtre des propriétés de l'appareil s'ouvrira.

3. Sous l'onglet **Avancés**, sélectionnez la section **Diagnostics à distance**.

Dans la fenêtre de diagnostic à distance de l'appareil, vous pouvez consulter le journal d'installation à distance de l'application.

Pour afficher le journal d'installation d'applications à distance sur un appareil :

1. Ouvrez la fenêtre de diagnostic à distance de l'appareil.
2. Sous l'onglet **Journaux d'événements**, dans le groupe **Fichiers de traçage**, cliquez sur le lien **Journaux d'installation à distance**.

   La fenêtre **Journaux d'événements de traçage de l'appareil** s'ouvre.

Pour plus d'informations sur le diagnostic à distance, consultez l'aide de Kaspersky Security Center.

Diagnostics à distance à l'aide de la Console d'administration

Si vous gérez l'application Kaspersky Endpoint Security via la Console d'administration, les diagnostics à distance sont effectués à l'aide de l'utilitaire spécial de diagnostic à distance de Kaspersky Security Center, qui est automatiquement installé sur l'appareil avec la Console d'administration.

Pour ouvrir la fenêtre principale de l'utilitaire de diagnostic des appareils distants :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil auquel vous souhaitez connecter l'utilitaire de diagnostic à distance, et dans le menu contextuel de l'appareil, sélectionnez **Outils externes → Diagnostics à distance**.

   La fenêtre principale de l'**utilitaire de diagnostic à distance Kaspersky Security Center** s'ouvrira.

À l'aide de l'utilitaire des diagnostics à distance de l'appareil, vous pouvez afficher le journal de l'installation à distance de l'application.

Pour afficher le journal d'installation d'applications à distance sur un appareil :

1. Ouvrez la fenêtre principale de l'utilitaire de diagnostic à distance de l'appareil.
2. Si nécessaire, configurez les paramètres de connexion de l'utilitaire à l'appareil. Dans la fenêtre principale de l'utilitaire de diagnostic à distance, cliquez sur le bouton **Connexion**.
3. Dans la fenêtre qui s'ouvre, dans l'arborescence des objets, sélectionnez le dossier **Journaux d'installation à distance**.

Pour en savoir plus sur l'utilitaire de diagnostic à distance, consultez l'aide de Kaspersky Security Center.

Annexes

Cette section contient des renseignements qui viennent compléter le contenu principal de l'aide.

Annexe 1. Fichiers de configuration et paramètres de l'application par défaut

Les fichiers de configuration suivants sont utilisés pour contrôler le fonctionnement de l'application Kaspersky Endpoint Security :

- Fichiers de configuration contenant les paramètres de configuration initiale de l'application :
- Fichiers de configuration prédéfinis créés automatiquement lors de la configuration initiale de l'application et contiennent les valeurs de paramètres spécifiées lors de la configuration initiale. Ces paramètres sont appliqués pendant l'exécution de l'application.
- Fichiers de configuration que vous pouvez créer à l'aide des commandes de gestion de l'application Kaspersky Endpoint Security. Ces fichiers de configuration peuvent contenir des paramètres de tâches et d'autres paramètres de l'application. Vous pouvez modifier ces fichiers et les importer dans l'application pour modifier les paramètres correspondants.

Règles d'édition des fichiers de configuration des tâches de l'application

Lors de la modification d'un fichier de configuration, veuillez respecter les règles suivantes :

- Attribuez une valeur à tous les paramètres obligatoires du fichier de configuration. Pour définir des paramètres distincts d'une tâche, vous pouvez opter pour la ligne de commande qui permet de réaliser l'opération sans fichier.
- Si le paramètre appartient à une section quelconque, ne le placez que dans cette section. Au sein d'une section, vous pouvez indiquer les paramètres dans n'importe quel ordre.
- Mettez les noms des sections entre crochets [ ].
- Spécifiez les valeurs des paramètres au format < `nom du paramètre` >=< `valeur du paramètre` > (les espaces entre le nom du paramètre et sa valeur ne sont pas traités).

  Exemple :

  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Les caractères "espace" et "tabulation" sont ignorés avant le premier guillemet et après le dernier guillemet d'une valeur de ligne, ainsi qu'au début et à la fin d'une valeur de ligne ne figurant pas entre guillemets.
- S'il s'avère nécessaire de définir plusieurs valeurs, répétez le paramètre autant de fois que le nombre de valeurs que vous voulez définir.

Exemple :

```
AreaMask.item_0000=*xml
AreaMask.item_0001=*doc
```

- Respectez la casse lors de la saisie des valeurs des paramètres des types suivants :
  - noms (masques) des objets analysés et des objets exclus ;
  - noms (masque) des menaces.

  Les autres valeurs de paramètres ne sont pas sensibles à la casse.
- Indiquez les valeurs des paramètres de type booléen comme suit : `Yes / No`.
- Les chaînes de valeur contenant un "espace" doivent être saisies entre guillemets (par exemple, les noms de fichiers ou les répertoires et les chemins d'accès à ceux-ci, les expressions contenant la date et l'heure au format AAAA-MM-DD HH:MM:SS).

  Les autres valeurs peuvent être saisies entre guillemets et sans guillemets.

  Exemple :

  ```
  AreaDesc=" Analyse des bases de messagerie "
  ```

  Un guillemet solitaire en début ou en fin de ligne est une erreur.

Fichiers de configuration initiale

Vous pouvez définir les paramètres de configuration initiale de l'application à l'aide d'un fichier de configuration :

- Si vous installez l'application à l'aide de Kaspersky Security Center, vous trouverez le fichier de configuration autoinstall.ini dans l'archive destinée à l'installation à distance de l'application. Vous pouvez définir les paramètres dans ce fichier avant de créer le paquet d'installation. Kaspersky Security Center applique ces paramètres lors de l'installation de l'application.
- Si vous installez l'application à l'aide de la ligne de commande, vous devez créer le fichier de configuration et indiquer son chemin d'accès lors du lancement de l'Assistant de configuration initiale. Vous pouvez copier la structure de ce fichier à partir du fichier de configuration autoinstall.ini.

Dans le fichier de configuration d'installation initiale, vous pouvez définir les paramètres indiqués dans le tableau ci-dessous. L'ensemble des paramètres applicables dépend de la manière dont l'application est utilisée. Les valeurs par défaut sont indiquées pour le fichier autoinstall.ini.

Les valeurs valides pour certains paramètres dépendent du type d'installation : à distance via Kaspersky Security Center ou via la ligne de commande.

Pour modifier un paramètre dans le fichier de configuration, indiquez sa valeur au format <nom du paramètre>=<valeur>.

Exemple

```
UPDATER_SOURCE=KLServers
```

Paramètre	Description	Valeurs

Section **[CustomSettings]**	Réglage fin de l'application pendant l'installation à distance. Permet de modifier certains paramètres du fichier kesl.ini ainsi que le niveau de traçage.
	
	Vous pouvez configurer l'application à l'aide de cette section uniquement lors de l'installation initiale.
	
	Si la section `[CustomSettings]` reprend les paramètres du fichier autoinstall.ini, les paramètres du fichier autoinstall.ini sont appliqués à l'application.
		• Tout paramètre du fichier de configuration kesl.ini au format <section de paramètres>.<nom du paramètre>=<valeur>
		Exemple
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel`, niveau de détail des fichiers de traçage de l'application :
		  • `Detailed` – crée un fichier de traçage détaillé de l'application.
		  • `MediumDetailed` – crée un fichier de traçage de l'application contenant des messages d'information et des messages d'erreur.
		  • `NotDetailed` – crée un fichier de traçage de l'application contenant des messages d'erreur.
		  • `None` (valeur par défaut) – ne crée pas de fichier de traçage de l'application.
		• `WdTraceLevel`, niveau de détail des fichiers de traçage du serveur Watchdog :
		  • `Detailed` pour générer un fichier de traçage détaillé du serveur Watchdog.
		  • `MediumDetailed` pour générer un fichier de traçage du serveur Watchdog contenant des messages d'information et des messages d'erreur.
		  • `NotDetailed` pour générer un fichier de traçage du serveur Watchdog contenant des messages d'erreur.
		  • `None` pour ne pas générer de fichier de traçage du serveur Watchdog.
		  • `Product` (valeur par défaut) pour définir une valeur égale à la valeur `TraceLevel`.

EULA_AGREED	Paramètre obligatoire. Acceptation des dispositions du Contrat de licence Utilisateur final.	`Yes` (valeur par défaut) : accepter les conditions du Contrat de licence utilisateur final. `No` : refuser les conditions du Contrat de licence utilisateur final. Cela entraîne l'interruption de l'installation de l'application.
PRIVACY_POLICY_AGREED	Paramètre obligatoire. Acceptation des dispositions de la Politique de confidentialité.	`Yes` (valeur par défaut) : accepter les conditions de la Politique de confidentialité. `No` : ne pas accepter les conditions de la Politique de confidentialité. Cela entraîne l'interruption de l'installation de l'application.

Paramètre	Description	Valeurs
USE_KSN	Paramètre obligatoire. Activation de l'utilisation de Kaspersky Security Network : Pour activer l'utilisation de KSN, vous devez accepter les termes de la Déclaration de Kaspersky Security Network. Si Kaspersky Endpoint Security est utilisé en mode standard et que vous avez activé l'utilisation de KSN, le mode cloud de l'application est automatiquement activé. Dans ce mode, Kaspersky Endpoint Security utilise une version allégée des bases de données des programmes malveillants.	`Yes` : accepter les conditions de la Déclaration de Kaspersky Security Network et activer l'utilisation de KSN. `No` (valeur par défaut) : ne pas accepter les conditions de la Déclaration de Kaspersky Security Network. La désactivation du KSN n'interrompt pas le processus d'installation de l'application.
LOCALE	Paramètres régionaux du service pour la localisation des événements de l'application envoyés à Kaspersky Security Center. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.	Les paramètres régionaux au format défini dans la RFC 3066. Valeurs possibles : • `de_DE.UTF-8` : Allemand ; • `en_US.UTF-8` – Anglais (États-Unis) • `es_MX.UTF-8` – Espagnol (Mexique) • `fr_FR.UTF-8` : Français ; • `ja_JP.UTF-8` : Japonais ; • `pt_BR.UTF-8` – Portugais (Brésil) • `ru_RU.UTF-8` : Russe ; • `zh_TW.UTF-8` : Chinois traditionnel. • `zh_CN.UTF-8` : Chinois simplifié ; Si le paramètre `LOCALE` n'est pas spécifié, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais (en_US.UTF-8 au format standard RFC 3066) est utilisé pour localiser les événements.

Paramètre	Description	Valeurs
INSTALL_LICENSE	Dans le fichier de configuration autoinstall.ini : le code d'activation permettant d'ajouter une clé de licence à l'application. Dans le fichier de configuration de la ligne de commande, vous pouvez également indiquer le chemin d'accès au fichier clé afin d'ajouter une clé de licence à l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`<activation code>` si vous souhaitez activer l'application à l'aide d'un code d'activation lors de l'installation via Kaspersky Security Center ou en ligne de commande. `<full path to key file>` si vous souhaitez activer l'application à l'aide d'un fichier clé lors de l'installation en ligne de commande. `None` : si vous n'avez pas besoin d'activer l'application lors de l'installation, par exemple, si l'application est installée dans un segment de réseau fermé sans accès à Internet.
UPDATER_SOURCE	Source des mises à jour des bases et des modules de l'application. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.	`SCServer` : le serveur d'administration de Kaspersky Security Center est la source des mises à jour. `KLServers` (par défaut) – utilise les serveurs de Kaspersky comme source de mise à jour. `<update source address>` sous la forme d'un répertoire local (par exemple, /home/bases) ou d'un serveur HTTP ou HTTPS distant (par exemple, http://example.com/bases/).
PROXY_SERVER	Adresse du serveur proxy à utiliser pour la connexion à Internet. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.	Adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de l'application lors de la configuration initiale. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.	`Yes` (valeur par défaut) : exécuter la tâche de mise à jour. `No` : ne pas lancer la tâche de mise à jour.

Paramètre	Description	Valeurs
KERNEL_SRCS_INSTALL	Compiler automatiquement le module du noyau au démarrage de la Protection contre les fichiers malicieux. Ce paramètre s'applique uniquement aux systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify.	`Yes` (valeur par défaut) : compiler le module du noyau lorsque la tâche de protection contre les fichiers malicieux démarre. `No` : ne pas compiler le module du noyau.
USE_GUI	Installation et utilisation de l'interface graphique de l'application. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.	`Yes` : installer et utiliser l'interface graphique de l'application (les fichiers d'installation de l'interface graphique doivent être ajoutés dans le paquet d'installation). `No` (valeur par défaut) : ne pas utiliser l'interface graphique.
GROUP_CLEAN	Paramètre obligatoire. Suppression automatique des utilisateurs des groupes privilégiés kesladmin et keslaudit avant l'installation de l'application.	`Yes` : supprimer les utilisateurs des groupes privilégiés. Si `Yes` est spécifié et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés. `No` (par défaut) – ne pas supprimer les utilisateurs des groupes privilégiés.
ADMIN_USER	Utilisateur auquel est attribué le rôle d'administrateur (admin). Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`.	
CONFIGURE_SELINUX	Configuration automatique de SELinux pour fonctionner avec l'application Kaspersky Endpoint Security.	`Yes` (valeur par défaut) : configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security. `No` – ne pas effectuer de configuration automatique de SELinux.
DISABLE_PROTECTION	Désactivation des modules fonctionnels d'une application après son installation. Une installation avec des modules désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si, après avoir installé l'application avec le paramètre `DISABLE_PROTECTION=Yes`, vous activez les modules nécessaires, alors après le redémarrage de l'application, les modules activés continueront de fonctionner.	`Yes` : désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation. `No` : ne pas désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation.

Paramètre	Description	Valeurs
ENDPOINT_AGENT_MODE	Utilisation de Kaspersky Endpoint Security en mode agent EDR. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` – Kaspersky Endpoint Security est utilisé en mode agent EDR pour prendre en charge les solutions Detection and Response de Kaspersky fonctionnant conjointement avec des solutions antivirus tierces sur les appareils protégés. `No` (valeur par défaut) : Kaspersky Endpoint Security est utilisé en mode standard ou en mode Light Agent (cf. le paramètre KSVLA_MODE).
EDR_EXPERT_CLOUD_MODE	Sélectionnez le mode du module Endpoint Detection and Response Expert. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` signifie que l'application utilise l'intégration de Kaspersky Endpoint Detection and Response Expert (cloud). `No` (valeur par défaut) signifie que l'application utilise l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises).
KSVLA_MODE	Utilisation de Kaspersky Endpoint Security en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` - Kaspersky Endpoint Security est utilisé en mode Light Agent (dans le cadre de Kaspersky Hybrid Cloud Security for Virtualization Light Agent). `No` (valeur par défaut) – Kaspersky Endpoint Security est utilisé en mode standard ou en mode agent EDR (cf. le paramètre ENDPOINT_AGENT_MODE).
SERVER_MODE	Le rôle de la machine virtuelle protégée (serveur ou poste de travail). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : la machine virtuelle protégée est utilisée comme serveur. `No` : la machine virtuelle protégée est utilisée comme poste de travail.

Paramètre	Description	Valeurs
VDI_MODE	Activation du mode de protection de l'infrastructure VDI pour optimiser les performances de l'application sur les machines virtuelles temporaires. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`Yes` : activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de Kaspersky Endpoint Security sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. `No` : ne pas activer le mode de protection de l'infrastructure VDI.
INTERCEPTOR_MODE	Le mécanisme d'interception des événements système utilisé par l'application Kaspersky Endpoint Security dans son travail. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`UseFanotify` (valeur par défaut) : utiliser la technologie fanotify pour intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.
INTERCEPTOR_FALLBACK_STRATEGY	L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`FallbackToFanotify` (valeur par défaut) : passer à l'utilisation de la technologie fanotify pour intercepter les événements système. `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système. Par conséquent, l'analyse des fichiers en temps réel n'est pas effectuée et le niveau de protection de l'appareil diminue.

Paramètre	Description	Valeurs
INTERCEPTOR_APPLY_STRATEGY	Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis. Ce paramètre s'applique uniquement lors de l'installation via Kaspersky Security Center. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`RestartServiceAutomatically` (valeur par défaut) : redémarrer automatiquement l'application pour exécuter le module de noyau mis à jour. `RestartServiceManually` : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur. Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.
ENABLE_TRACES_ON_FIRST_STARTUP	Créer un fichier de traçage de l'application lors du premier lancement après l'installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.	`Yes` : créer un fichier de traçage de l'application lors du premier lancement après l'installation. `No` (valeur par défaut) – ne pas créer de fichier de traçage au premier démarrage de l'application.
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	Utiliser le mode d'installation de l'application qui ignore les erreurs du gestionnaire de paquets. Ce mode peut être utilisé si l'application n'a pas pu être installée normalement. Ce paramètre s'applique uniquement lors de l'installation via Kaspersky Security Center. Il est conseillé de modifier les valeurs par défaut en suivant les instructions du Support technique.	`No` (valeur par défaut) pour installer l'application normalement. `Yes` pour installer l'application tout en ignorant les erreurs système.

Paramètre	Description	Valeurs
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	Supprimer automatiquement le paquet d'installation de l'application s'il n'a été installé que partiellement. Désactivez ce paramètre si l'application n'a pas pu être installée normalement. Ce paramètre s'applique uniquement lors de l'installation via Kaspersky Security Center. Il est conseillé de modifier les valeurs par défaut en suivant les instructions du Support technique.	`Yes` (valeur par défaut) pour supprimer le paquet d'installation de l'application partiellement installé. `No` pour installer l'application en ignorant le paquet installé partiellement.
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	Activer les journaux de débogage des gestionnaires de paquets. Ce paramètre peut être utilisé si l'application n'a pas pu être installée normalement. Ce paramètre s'applique uniquement lors de l'installation via Kaspersky Security Center. Il est conseillé de modifier les valeurs par défaut en suivant les instructions du Support technique.	`Yes` pour activer les journaux de débogage des gestionnaires de paquets. `No` (valeur par défaut) pour ne pas activer les journaux de débogage des gestionnaires de paquets.

Paramètres de configuration initiale dans le paquet d'installation

Vous pouvez spécifier les paramètres de configuration initiale de l'application dans le paquet d'installation que vous utilisez pour installer l'application à l'aide de Kaspersky Security Center.

Dans Kaspersky Security Center Web Console, vous pouvez spécifier les paramètres de configuration initiaux de l'application Kaspersky Endpoint Security dans les propriétés du paquet d'installation sous l'onglet **Paramètres**. Les paquets d'installation créés sont disponibles dans la fenêtre principale de Web Console dans l'une des sections suivantes :

- **Découverte et déploiement des appareils → Déploiement et attribution → Paquets d'installation**.
- **Opérations → Stockages → Paquets d'installation**.

Dans la Console d'administration de Kaspersky Security Center, vous pouvez spécifier les paramètres de configuration initiale de l'application Kaspersky Endpoint Security lors de la création d'un paquet d'installation ou dans les propriétés du paquet d'installation dans la section **Paramètres**. Les paquets d'installation créés sont accessibles dans l'arborescence de la Console d'administration dans le dossier **Avancés → Installation à distance → Paquets d'installation**.

L'ensemble des paramètres applicables dépend de la manière dont l'application est utilisée.

Paramètres de configuration initiale dans Web Console

Paramètres de la configuration initiale de l'application

Paramètre	Description
Mode d'utilisation	• **Mode standard pour protéger les postes de travail et les serveurs** (valeur par défaut). Si cette option est sélectionnée, l'application est utilisée comme une application autonome pour protéger les postes de travail et les serveurs exécutant des systèmes d'exploitation Linux. • **Endpoint Detection and Response Agent**. Si cette option est sélectionnée, l'application permet la collaboration entre les solutions Detection and Response de Kaspersky et les solutions antivirus tierces sur les appareils protégés. • **Light Agent pour protéger les environnements virtuels**. Si cette option est sélectionnée, l'application est utilisée en mode Light Agent (dans le cadre de Kaspersky Security for Virtualization Light Agent). Les modes EDR Agent et Light Agent ne sont pas disponibles pour les appareils équipés d'un processeur Elbrus.
Activer Endpoint Detection and Response Expert (cloud)	Cochez la case pour utiliser l'intégration avec Endpoint Detection and Response Expert (cloud). En mode standard, l'application prend en charge l'intégration avec Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises). Si cette case est décochée, l'intégration avec Endpoint Detection and Response Expert (on-premises) est utilisée. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Activer le mode de protection de l'infrastructure VDI	Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
La machine virtuelle protégée est utilisée comme serveur	Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. Par défaut, la case est cochée (la machine virtuelle est utilisée dans l'infrastructure virtuelle comme serveur). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.

Paramètre	Description
Langue des événements dans KSC	Langue de localisation des événements de l'application envoyés à Kaspersky Security Center : • **Système** (valeur par défaut) : la langue de localisation du système d'exploitation. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais est utilisé pour localiser les événements. • Une des langues prises en charge par Kaspersky Endpoint Security : anglais (États-Unis), espagnol (Mexique), chinois traditionnel, chinois simplifié, allemand, portugais (Brésil), russe, français, japonais. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.
Activer l'application	Cochez cette case si vous souhaitez activer l'application lors de l'installation. Saisissez le code d'activation dans le champ qui s'ouvre. La case est décochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Sources de mises à jour	Source des mises à jour des bases et des modules de l'application. • **Serveurs de mise à jour de Kaspersky** (valeur par défaut). • **Kaspersky Security Center**. • **Autres sources sur le réseau local ou sur Internet**. Si vous sélectionnez cette option, saisissez l'adresse de la source de mises à jour dans le champ qui s'ouvre. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Exécuter la tâche de mise à jour des bases après l'installation	Si la case est cochée, après l'installation de l'application, la tâche de mise à jour des bases de données et des modules de l'application est lancée. La case est cochée par défaut. Décochez cette case si vous avez ajouté au paquet d'installation les bases de l'application préalablement téléchargées. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Indiquer les paramètres du serveur proxy	Cochez cette case si vous utilisez un serveur proxy pour accéder à Internet. Dans le champ qui s'ouvre, saisissez l'adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.

Paramètre	Description
Installer le code source du noyau	Si la case est cochée, pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, lorsque la protection contre les fichiers malicieux est lancée, la compilation du module du noyau est automatiquement démarrée. La case est cochée par défaut. Ce paramètre s'applique uniquement aux systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Utiliser l'interface graphique	Cochez cette case si vous prévoyez d'installer et d'utiliser l'interface graphique de l'application. Les fichiers d'installation de l'interface graphique doivent être ajoutés au paquet d'installation. La case est décochée par défaut. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Indiquer un utilisateur ayant le rôle d'administrateur (admin)	Cochez la case si vous voulez spécifier l'utilisateur auquel attribuer le rôle d'administrateur (admin). Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`. Dans le champ qui s'ouvre, saisissez le nom d'utilisateur.
Configurer automatiquement SELinux	Si cette case est cochée, SELinux est automatiquement configuré pour fonctionner avec Kaspersky Endpoint Security lors de la configuration initiale de l'application. La case est cochée par défaut.
Supprimer les utilisateurs des groupes privilégiés	Cochez la case pour supprimer automatiquement les utilisateurs des groupes privilégiés kesladmin et keslaudit avant d'installer l'application. La case est décochée par défaut. Si la case est cochée et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.
Désactiver les modules de protection et les tâches d'analyse lors du premier lancement de l'application après l'installation	Cochez la case si vous souhaitez exécuter l'application avec les module de protection et les tâches d'analyse désactivés après l'installation. Une installation avec des modules de protection désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si vous activez les modules et les tâches nécessaires, alors après le redémarrage de l'application, les modules et les tâches activés continueront de fonctionner.
Activer le traçage lorsque l'application est lancée pour la première fois après l'installation	Cochez cette case si vous souhaitez activer la création d'un fichier de traçage lors du premier lancement de l'application après son installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.
Mécanisme d'interception	Le mécanisme d'interception des événements système utilisé par l'application dans son travail : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, un module de noyau mis à jour est installé lors de l'installation de l'application. L'application utilise ce module pour intercepter les événements système. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.

Paramètre	Description
Si le module de noyau mis à jour ne parvient pas à démarrer	Action que l'application exécute si le module de noyau mis à jour ne parvient pas à démarrer : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Activer le mode d'ignorance des erreurs du gestionnaire de paquets	Cochez cette case pour ignorer les erreurs du gestionnaire de paquets lors de l'installation de l'application. La case est décochée par défaut. Ce paramètre peut être utilisé si l'application n'a pas pu être installée normalement. Nous vous recommandons de n'activer ce paramètre que sous la supervision du Support technique

Paramètres de configuration initiale dans la Console d'administration

Paramètres de la configuration initiale de l'application

Paramètre	Description
Langue des événements dans KSC	Langue de localisation des événements de l'application envoyés à Kaspersky Security Center : • **Système** (valeur par défaut) : la langue de localisation du système d'exploitation. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais est utilisé pour localiser les événements. • Une des langues prises en charge par Kaspersky Endpoint Security : anglais (États-Unis), espagnol (Mexique), chinois traditionnel, chinois simplifié, allemand, portugais (Brésil), russe, français, japonais. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.
Code d'activation	Si vous souhaitez activer l'application lors de l'installation, saisissez le code d'activation. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Sélectionner la source de mise à jour	En cliquant sur le bouton **Configurer**, une fenêtre s'ouvre dans laquelle vous pouvez sélectionner la source de mise à jour des bases et modules d'application : • **Serveurs de mises à jour Kaspersky** (valeur par défaut). • **Kaspersky Security Center**. • **Autre source sur le réseau local ou sur Internet**. Si vous sélectionnez cette option, saisissez l'adresse de la source de mise à jour dans le champ **Adresse**. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.

Paramètre	Description
Exécuter la tâche de mise à jour des bases après l'installation	Si la case est cochée, après l'installation de l'application, la tâche de mise à jour des bases de données et des modules de l'application est lancée. La case est cochée par défaut. Décochez cette case si vous avez ajouté au paquet d'installation les bases de l'application préalablement téléchargées. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Adresse du serveur proxy	Si vous utilisez un serveur proxy pour accéder à Internet, saisissez l'adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. Lorsque vous indiquez une adresse IPv6, saisissez-la entre crochets. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Installer le code source du noyau	Si la case est cochée, pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, lorsque la protection contre les fichiers malicieux est lancée, la compilation du module du noyau est automatiquement démarrée. La case est cochée par défaut. Ce paramètre s'applique uniquement aux systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Utiliser l'interface utilisateur graphique	Cochez cette case si vous prévoyez d'installer et d'utiliser l'interface graphique de l'application. Les fichiers d'installation de l'interface graphique doivent être ajoutés au paquet d'installation. La case est décochée par défaut. Ce paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode agent EDR.
Utilisateur avec rôle d'administrateur (admin)	Nom de l'utilisateur auquel vous souhaitez attribuer le rôle d'administrateur. Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`.
Configurer automatiquement SELinux	Si cette case est cochée, SELinux est automatiquement configuré pour fonctionner avec Kaspersky Endpoint Security lors de la configuration initiale de l'application. La case est cochée par défaut.
Supprimer les utilisateurs des groupes privilégiés	Cochez la case pour supprimer automatiquement les utilisateurs des groupes privilégiés kesladmin et keslaudit avant d'installer l'application. La case est décochée par défaut. Si la case est cochée et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.
Désactiver les modules de protection et les tâches d'analyse la première fois que vous lancez l'application après l'installation	Cochez la case si vous souhaitez exécuter l'application avec les module de protection et les tâches d'analyse désactivés après l'installation. Une installation avec des modules de protection désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si vous activez les modules et les tâches nécessaires, alors après le redémarrage de l'application, les modules et les tâches activés continueront de fonctionner.

Paramètre	Description
Activer le traçage des applications au premier lancement après l'installation	Cochez cette case si vous souhaitez activer la création d'un fichier de traçage lors du premier lancement de l'application après son installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.
Mode d'utilisation de l'application	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Mode d'utilisation de l'application**. Cette fenêtre permet de sélectionner un mode pour l'application. • **Mode standard pour protéger les postes de travail et les serveurs** (valeur par défaut). Si cette option est sélectionnée, l'application est utilisée comme une application autonome pour protéger les postes de travail et les serveurs exécutant des systèmes d'exploitation Linux. • **Endpoint Detection and Response Agent**. Si cette option est sélectionnée, l'application permet la collaboration entre les solutions Detection and Response de Kaspersky et les solutions antivirus tierces sur les appareils protégés. • **Light Agent pour protéger les environnements virtuels**. Si cette option est sélectionnée, l'application est utilisée en mode Light Agent (dans le cadre de Kaspersky Security for Virtualization Light Agent). Les modes EDR Agent et Light Agent ne sont pas disponibles pour les appareils équipés d'un processeur Elbrus.
Activer Endpoint Detection and Response Expert (cloud)	Cochez la case pour utiliser l'intégration avec Endpoint Detection and Response Expert (cloud). En mode standard, l'application prend en charge l'intégration avec Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises). Si cette case est décochée, l'intégration avec Endpoint Detection and Response Expert (on-premises) est utilisée. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
La machine virtuelle protégée est utilisée comme serveur	Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. Par défaut, la case est cochée (la machine virtuelle est utilisée dans l'infrastructure virtuelle comme serveur). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Activer le mode de protection de l'infrastructure VDI	Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.

Paramètre	Description
Interception des événements système	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Paramètres d'interception des événements système**. Dans cette fenêtre, vous pouvez sélectionner le mode d'interception des événements système à utiliser par l'application : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, un module de noyau mis à jour est installé lors de l'installation de l'application. L'application utilise ce module pour intercepter les événements système. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Si le module de noyau mis à jour ne parvient pas à démarrer (fenêtre **Paramètres d'interception des événements système**)	Action que l'application exécute si le module de noyau mis à jour ne parvient pas à démarrer : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.
Activer le mode d'ignorance des erreurs du gestionnaire de paquets	Cochez cette case pour ignorer les erreurs du gestionnaire de paquets lors de l'installation de l'application. La case est décochée par défaut. Ce paramètre peut être utilisé si l'application n'a pas pu être installée normalement. Nous vous recommandons de n'activer ce paramètre que sous la supervision du Support technique

Fichiers de configuration préinstallés

Après la configuration initiale, les fichiers de configuration suivants sont créés dans l'application :

- /var/opt/kaspersky/kesl/common/objects-backup/

  Le fichier de configuration agreements.ini contient les paramètres relatifs au Contrat de licence utilisateur final, à la Politique de confidentialité et à la Déclaration de Kaspersky Security Network.

- /var/opt/kaspersky/kesl/common/kesl.ini

  Le fichier de configuration kesl.ini contient les paramètres figurant dans le tableau ci-dessous.

Si nécessaire, vous pouvez modifier les valeurs des paramètres dans le fichier kesl.ini.

Il est conseillé de modifier les valeurs par défaut dans ces fichiers uniquement en suivant les instructions des experts du Support technique.

Pour appliquer les modifications apportées au fichier de configuration, redémarrez l'application Kaspersky Endpoint Security.

Si le paramètre est absent dans le fichier ou si une valeur incorrecte du paramètre est spécifiée, l'application utilisera la valeur par défaut.

Paramètres du fichier de configuration kesl.ini

Paramètre	Description	Valeurs
La section **[Général]** contient les paramètres suivants :		
`Locale`	Paramètres régionaux utilisés pour localiser les événements transmis par l'application Kaspersky Endpoint Security à Kaspersky Security Center. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.	La locale au format défini par la norme RFC 3066. Si le paramètre `Locale` n'est pas spécifié, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais (en_US.UTF-8 au format standard RFC 3066) est utilisé pour localiser les événements.
`PackageType`	Format du progiciel installé. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. La valeur est renseignée automatiquement lors de la configuration initiale de l'application.	`rpm` : un paquet RPM est installé. `deb` : un paquet DEB est installé.
`UseFanotify`	Utilisation de la technologie fanotify pour intercepter les opérations sur les fichiers. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : l'application utilise la technologie fanotify pour intercepter les opérations sur les fichiers. `false/no` : la technologie fanotify n'est pas utilisée.
`KsvlaMode`	Utilisation de Kaspersky Endpoint Security en mode Light Agent. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` signifie que l'application est utilisée en mode Light Agent. `false/no` : l'application est utilisée en mode standard.

Paramètre	Description	Valeurs
`EndpointAgentMode`	Utilisation de Kaspersky Endpoint Security en mode agent EDR. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` signifie que l'application est utilisée en mode EDR Agent. `false/no` : l'application est utilisée en mode standard.
`KcsMode`	Utilisation de l'application Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Container Security en tant que module Protection contre les fichiers malicieux. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Ce paramètre est utilisé uniquement dans le fonctionnement de la solution Kaspersky Container Security. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : l'application est utilisée comme module Protection contre les fichiers malicieux dans la solution Kaspersky Container Security. `false/no` (par défaut) signifie que l'application est utilisée dans l'un des modes de Kaspersky Endpoint Security (mode standard, mode EDR Agent ou mode Light Agent).
`StartupTraces`	Activation de la création de fichiers de traçage au lancement de l'application.	`true/yes` : crée des fichiers de traçage au lancement de l'application. `false/no` (valeur par défaut) : ne crée pas de fichiers de traçage au lancement de l'application.
`RevealSensitiveInfoInTraces`	Affichage des informations dans les fichiers de traçage qui peuvent contenir des données personnelles (par exemple, des mots de passe).	`true/yes` : afficher des informations pouvant contenir des données personnelles dans les fichiers de traçage de l'application. `false/no` (valeur par défaut) : ne pas afficher d'informations pouvant contenir des données personnelles dans les fichiers de traçage.
`AsyncTraces`	Activation du traçage asynchrone, dans lequel les informations sont écrites pour tracer les fichiers de manière asynchrone.	`true/yes` : activer le traçage asynchrone. `false/no` (par défaut) : ne pas activer le traçage asynchrone.
`MinFreeDiskSpace`	Quantité minimale de mémoire disque qui restera après l'écriture du fichier de vidage, en mégaoctets.	Valeur par défaut : 300.
`ScanMemoryLimit`	Limite d'utilisation de la RAM par l'application en mégaoctets.	Valeur par défaut : 8192. Il est recommandé de définir la valeur du paramètre `ScanMemoryLimit` à une valeur inférieure à celle du paramètre `MaxMemory` afin d'éviter que les tâches d'analyse et les redémarrages de l'application n'utilisent toute la mémoire disponible.
`MachineId`	ID unique de l'appareil de l'utilisateur.	La valeur du paramètre est renseignée automatiquement lors de l'installation de l'application.
`SocketPath`	Chemin d'accès au socket pour la connexion à distance, par exemple, de l'interface graphique et de l'utilitaire kesl-control.	Valeur par défaut : /var/run/bl4control.
`MaxInotifyWatches`	Limitation du nombre d'abonnements aux modifications de fichiers et de répertoires (user watches) indiqué dans /proc/sys/fs/inotify/max_user_watches. Si la valeur du paramètre du système d'exploitation est inférieure à la valeur du paramètre `MaxInotifyWatches`, l'application remplace la valeur du paramètre du système d'exploitation par la valeur du paramètre `MaxInotifyWatches`.	Valeur par défaut : 299987.

Paramètre	Description	Valeurs
`MaxInotifyInstances`	Limitation du nombre d'abonnements aux modifications des fichiers et des répertoires par utilisateur, spécifiée dans le fichier /proc/sys/fs/inotify/max_user_instances. Si la valeur du paramètre du système d'exploitation est inférieure à la valeur du paramètre `MaxInotifyInstances`, l'application remplace la valeur du paramètre du système d'exploitation par la valeur du paramètre `MaxInotifyInstances`.	Valeur par défaut : 4047.
`ExecEnvMax`	Nombre de variables d'environnement que l'application capturera à partir de l'appel de la commande.	Valeur par défaut : 50.
`ExecArgMax`	Nombre d'arguments que l'application récupérera à partir de l'appel exec.	Valeur par défaut : 20.
`AdditionalDNSLookup`	Utilisation du DNS public. Si l'accès aux serveurs via le DNS système échoue, l'application utilisera le DNS public. Ceci est nécessaire pour la mise à jour des bases de l'application et maintenir le niveau de sécurité de l'appareil. L'application utilisera les DNS publics suivants par ordre d'apparition : 1. Google Public DNS™ (8.8.8.8). 2. Cloudflare® DNS (1.1.1.1). 3. Alibaba Cloud® DNS (223.6.6.6). 4. Quad9® DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).	`true/yes` : utiliser le DNS public pour accéder aux serveurs de Kaspersky. `false/no` (valeur par défaut) : ne pas utiliser le DNS public pour accéder aux serveurs de Kaspersky. Les demandes de l'application peuvent contenir des adresses de domaine et l'adresse IP externe de l'utilisateur, car l'application établit une connexion TCP/UDP avec le serveur DNS. Ces données sont nécessaires, par exemple, pour l'analyse du certificat d'une ressource Internet lors de l'accès via HTTPS. Si l'application utilise un serveur DNS public, les règles de traitement des données sont régies par la Politique de confidentialité de ce service.
`PanicThreshold`	Nombre maximal d'arrêts anormaux de l'application lors de l'utilisation d'un module de noyau mis à jour. Lorsque la valeur spécifiée est atteinte, l'application passe en mode « sécurisé », dans lequel le module du noyau mis à jour n'est pas lancé. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	Valeur par défaut : 3.
`SafeMode`	Activation du mode « sécurisé » lors de l'utilisation du module de noyau mis à jour. Dans ce mode, l'application n'exécute pas le module de noyau mis à jour. Le mode « sécurisé » est activé automatiquement si l'application atteint le nombre maximal d'arrêts anormaux spécifié dans le paramètre `PanicThreshold`. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : le mode de fonctionnement « sécurisé » de l'application est activé. `false/no` (valeur par défaut) : le mode « sécurisé » de l'application est désactivé, l'application fonctionne en mode normal.

Paramètre	Description	Valeurs
`GetContainerName`	Transmission des informations suivantes relatives aux conteneurs dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response : • indicateur précisant que l'événement s'est produit dans un conteneur ; • identifiant de l'espace de noms du conteneur ; • nom du conteneur. Le nom du conteneur n'est transmis que si vous disposez d'une licence pour utiliser la tâche Analyse du conteneur et si le conteneur a une durée de vie suffisante. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` (valeur par défaut) : transmettre des informations étendues sur le conteneur dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response. `false/no` : ne pas transmettre les informations étendues du conteneur dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response.
`UseIncreasedXdrEventsCache`	Gestion du cache des événements lors de l'intégration aux solutions Detection and Response. Il existe un compromis entre performances élevées et consommation de RAM.	`true/yes` (valeur par défaut) minimise les E/S disque, mais utilise davantage de RAM (100 Mo). `false/no` utilise moins de mémoire (environ 5 Mo) au prix d'un plus grand nombre d'opérations de lecture et d'écriture sur le disque.
`FastShutdown`	Arrêt rapide du processus kesl lors de l'arrêt ou du redémarrage de l'application.	`true/yes` active l'arrêt rapide du processus kesl lors de l'arrêt de l'application. `false/no` (valeur par défaut) désactive l'arrêt rapide du processus kesl lors de l'arrêt de l'application.
La section **[Network]** contient les paramètres suivants :		
`WtpFwMark`	Étiquette dans les règles de l'utilitaire iptables pour rediriger le trafic vers une application en vue de son traitement par le module Protection contre les menaces Internet. Vous devrez peut-être modifier cette étiquette si un autre logiciel s'exécute sur le même appareil que l'application installée, que ce logiciel utilise le neuvième bit du masque de paquet TCP et qu'un conflit se produit.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x100. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x1000 ou 0x10000 (la marque est limitée à un entier de 32 bits).
`NtpFwMark`	Étiquette dans les règles de l'utilitaire iptables pour rediriger le trafic vers une application en vue de son traitement par le module Protection contre les menaces réseau. Vous devrez peut-être modifier cette étiquette si un autre logiciel s'exécute sur le même appareil que l'application installée, que ce logiciel utilise le neuvième bit du masque de paquet TCP et qu'un conflit se produit.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x200. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x2000 ou 0x20000 (la marque est limitée à un entier de 32 bits).

Paramètre	Description	Valeurs
`BypassFwMark`	Étiquette qui marque les paquets créés ou analysés par l'application afin qu'ils ne tombent pas à nouveau dans le programme pour analyse.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x400. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x4000 ou 0x40000 (la marque est limitée à un entier de 32 bits).

`BypassNFlogMark`	Marque des paquets que l'application ignorera lors de l'analyse.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x.
		Valeur par défaut : 0x800.
		Exemples :
		Ignorer tout le trafic TCP avec l'appareil spécifié :
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		Ignorer le trafic du serveur HTTPS :
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x8000 ou 0x80000 (la marque est limitée à un entier de 32 bits).

`ProxyRouteTable`	Numéro de table de routage.	Valeur par défaut : 101.
La section **[ScannerImpactStats]** contient les paramètres suivants :		
`CollectFileScanStatistics`	Permet à l'application de comptabiliser les statistiques de vérification des fichiers et des processus.	`true/yes` (valeur par défaut) : active le calcul des statistiques de l'analyse des fichiers et des processus. `false/no` : ne pas activer le calcul des statistiques de l'analyse des fichiers et des processus.
`StatCollectionPeriod`	Intervalle de temps pendant lequel l'application comptabilise les statistiques des fichiers vérifiés et des processus détectés avant de les enregistrer dans le fichier de traçage et dans les rapports.	Valeur par défaut : 10 minutes.
`StatCollectionCount`	Nombre de fichiers vérifiés et de processus détectés qui ont été comptés par l'application pendant l'intervalle de temps spécifié par le paramètre `StatCollectionPeriod` et qui seront inclus dans le rapport et dans les fichiers de traçage.	Valeur par défaut : 10.
`ReportStatAmount`	Nombre d'enregistrements qui seront affichés dans les rapports sur les fichiers et les processus les plus fréquemment analysés par jour.	Valeur par défaut : 20.
La section **[Virtualization]** contient les paramètres suivants :		

Paramètre	Description	Valeurs
`ServerMode`	Rôle de la machine virtuelle protégée sur laquelle Kaspersky Endpoint Security est utilisé en mode Light Agent : serveur ou poste de travail. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : la machine virtuelle est utilisée comme serveur. `false/no` : la machine virtuelle est utilisée comme poste de travail.
`VdiMode`	Active le mode de protection de l'infrastructure VDI lors de l'utilisation de l'application en mode Light Agent. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : le mode de protection de l'infrastructure VDI est activé. `false/no` : le mode de protection de l'infrastructure VDI est désactivé.
La section **[Watchdog]** contient les paramètres suivants :		
`TimeoutAfterHeadshot`	Temps d'attente maximal pour que le processus kesl se termine à partir du moment où le signal HEADSHOT est envoyé par le serveur Watchdog au processus kesl.	Valeur par défaut : 2 minutes.
`StartupTimeout`	Le temps d'attente maximum pour démarrer l'application (en minutes), après quoi le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 3 minutes.
`TimeoutAfterKill`	Temps d'attente maximal pour que le processus kesl géré termine son exécution à partir du moment où le serveur Watchdog envoie le signal SIGKILL au processus kesl. Si le processus kesl n'a pas terminé son exécution après ce délai, l'action spécifiée par le paramètre --failed-kill est exécutée.	Valeur par défaut : 2 jours.
`PingInterval`	Fréquence à laquelle l'application tente d'envoyer un message PONG au serveur Watchdog en réponse à un message PING reçu.	Valeur par défaut : 2000 millisecondes.
`MaxRestartCount`	Nombre maximum de tentatives consécutives infructueuses pour lancer l'application.	Valeur par défaut : 5.
`ActivityTimeout`	Intervalle de temps maximum pendant lequel l'application doit envoyer un message au serveur Watchdog. S'il n'y a pas de message de l'application pendant cet intervalle de temps, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 2 minutes.
`ConnectTimeout`	Le temps maximum d'attente pour qu'une application se connecte au serveur Watchdog à partir du moment où le processus kesl démarre. Si l'application n'a pas le temps de créer une connexion dans cet intervalle de temps, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 3 minutes.

Paramètre	Description	Valeurs
`RegisterTimeout`	Intervalle de temps maximum à partir du moment où l'application se connecte au serveur Watchdog jusqu'à ce que le serveur reçoive le message REGISTER.	Valeur par défaut : 500 millisecondes.
`TimeoutAfterShutdown`	Temps d'attente maximal pour que le processus kesl se termine à partir du moment où le signal SHUTDOWN est envoyé par le serveur Watchdog au processus kesl.	Valeur par défaut : 2 minutes.
`MaxMemory`	Limite d'utilisation de la mémoire résidente du processus kesl. Si la mémoire résidente du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	`off` : l'utilisation de la mémoire résidente n'est pas limitée. `<value>%` – valeur comprise entre 1 et 100 % de la mémoire RAM. `<value>MB` – valeur en mégaoctets. `lowest/<value>%/<value>MB` – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. `highest/<value>%/<value>MB` – la plus grande des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. `auto` : jusqu'à 50 % de la mémoire disponible, mais pas moins de 2 Go et pas plus de 16 Go. Valeur par défaut : `auto`.
`MaxVirtualMemory`	Limite d'utilisation de la mémoire virtuelle du processus kesl. Si la mémoire virtuelle du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	`off` (valeur par défaut) : l'utilisation de la mémoire virtuelle n'est pas limitée. `<value>MB` – valeur en mégaoctets.
`MaxSwapMemory`	Limite de taille du fichier swap du processus kesl. Si le fichier swap du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	`off` (valeur par défaut) – La taille du fichier swap n'est pas limitée. `<value>%` – valeur comprise entre 0 et 100 % de la mémoire RAM. `<value>MB` – valeur en mégaoctets. `lowest/<value>%/<value>MB` – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. `highest/<value>%/<value>MB` – la plus grande des deux : la valeur en pourcentage et la valeur absolue en mégaoctets.
`TrackProductCrashes`	Activation d'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center lorsque l'application est instable.	`true/yes` : activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center. `false/no` (valeur par défaut) : désactiver l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.
`ProductHealthLogFile`	Chemin d'accès au fichier utilisé pour surveiller la stabilité de l'application.	Valeur par défaut : /var/opt/kaspersky/kesl/private/kesl_health.log.
`WarnThreshold`	L'intervalle de temps (en secondes) pendant lequel l'application doit compter le nombre d'arrêts anormaux avant d'afficher une notification instable.	Valeur par défaut : 3600 secondes.
`WarnAfter_#_crash`	Le nombre maximum d'arrêts anormaux de l'application, une fois atteint, une notification concernant le fonctionnement instable de l'application s'affiche.	Valeur par défaut : 10. Si la valeur est 0, la notification d'instabilité de l'application ne s'affiche pas.
`WarnRemovingThreshold`	Intervalle de temps (en secondes) après lequel l'état instable de l'application sera effacé.	Valeur par défaut : 86400 secondes.
`SyscallHangProbePeriod`	Fréquence à laquelle le serveur Watchdog appelle les fonctions système open et execve et augmente les compteurs pour les appels réussis de ces fonctions.	Valeur par défaut : 3 secondes.

Paramètre	Description	Valeurs
`SyscallHangCheckPeriod`	Fréquence à laquelle le serveur Watchdog vérifie les compteurs pour les appels réussis des fonctions open et execve. Si passé ce délai la valeur des compteurs n'a pas changé, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 32 secondes.
`DumpSuspendPeriod`	Temps maximum d'attente pour la création du fichier de vidage de l'application avant que le serveur Watchdog ne suspende la vérification de l'activité de l'application. Si passé ce délai; la création du fichier de vidage n'est pas terminée, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeurs possibles : 1 – 30 minutes. Valeur par défaut : 2 minutes.
`TimeoutAfterCoredump`	Durée maximale pendant laquelle le serveur Watchdog suspendra l'envoi d'autres signaux au processus kesl après l'envoi d'un signal SIGTRAP, lequel est envoyé lors de la procédure d'arrêt anormal du processus.	Valeur par défaut : 2 minutes. Il est recommandé de spécifier une valeur du paramètre `TimeoutAfterCoredump` supérieure ou égale à la valeur du paramètre `DumpSuspendPeriod`. Vous pouvez spécifier la valeur du paramètre dans les unités suivantes : • pendant `<n> day|days|d` jours • pendant `<n> hour|hours|hr|h` heures • pendant `<n> minute|minutes|min|m` minutes • pendant `<n> second|seconds|sec|s` secondes • pendant `<n> [msec|ms]` millisecondes Si aucune unité n'est spécifiée, l'application utilisera par défaut les millisecondes.
`TimeoutMaxCleanPeriod`	Durée maximale accordée au processus qui efface les règles du pare-feu du système d'exploitation. Si le processus ne signale pas son achèvement dans ce délai, le serveur Watchdog considère que le processus est bloqué.	Valeur par défaut : 10 secondes.
`TimeoutAfterClean`	Durée maximale accordée au processus qui efface les règles du pare-feu du système d'exploitation pour se terminer après l'envoi du signal SIGTERM au processus de nettoyage par le serveur Watchdog.	Valeur par défaut : 10 secondes.
La section **[Environment]** n'est pas présente dans le fichier de configuration par défaut.		
`ExperimentalContainerdSupport`	Activation de la prise en charge de l'environnement containerd lors du fonctionnement du module Surveillance du conteneur. Ce paramètre n'est pas présent dans le fichier de configuration par défaut. Si vous souhaitez utiliser l'environnement containerd lors de l'exécution du module Surveillance du conteneur, vous devez ajouter manuellement la section `[Environment]` au fichier de configuration et y ajouter le paramètre `ExperimentalContainerdSupport`. Ce paramètre ne s'applique pas aux appareils équipés d'un processeur Elbrus.	`true/yes` : activer la prise en charge de l'environnement containerd lors du fonctionnement du module Surveillance du conteneur. `false/no` : ne pas activer la prise en charge de l'environnement containerd lors du fonctionnement du module Surveillance du conteneur.

Paramètre	Description	Valeurs
`ReduceSWMemoryConsumption`	Limitation de la consommation de mémoire par le module Détection comportementale pour le traitement de la file d'attente des événements. La définition d'une limite de mémoire a un impact négatif sur la détection des menaces, notamment sur la qualité de la télémétrie transmise dans le cadre de l'intégration avec des solutions Detection and Response. Nous recommandons de définir une limite uniquement sur les systèmes fortement sollicités et après avoir contacté le Support technique afin d'obtenir des instructions spécifiques, s'il n'existe aucune autre option pour résoudre le problème de consommation élevée de mémoire.	1 – limite l'utilisation de la mémoire par le module Détection comportementale pour le traitement de la file d'attente des événements. 0 (par défaut) – ne limite pas l'utilisation de la mémoire. Le relancement de l'application est nécessaire après la modification de ce paramètre.

Paramètres des tâches de ligne de commande par défaut

Cette section contient les paramètres par défaut de toutes les tâches prédéfinies fournies pour gérer l'application Kaspersky Endpoint Security à l'aide de la ligne de commande.

Les tâches `Rollback` et `License` n'ont aucun paramètre.

Paramètres par défaut de la tâche File_Threat_Protection (ID:1)

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No
```

```
ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Scan_My_Computer (ID:2)

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No
```

```
ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Scan_File (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Critical_Areas_Scan (ID:4)

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0
```

```
QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut pour la tâche Update (ID:6)

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

Paramètres par défaut de la tâche System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Paramètres par défaut de la tâche Anti_Cryptor (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Web_Threat_Protection (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Paramètres par défaut de la tâche Device_Control (ID:15)

```
OperationMode=Block

AllowToRequestTemporaryAccess=No

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus
```

```
ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes
```

```
ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Paramètres par défaut de la tâche Removable_Drives_Scan (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Paramètres par défaut de la tâche Network_Threat_Protection (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Paramètres par défaut pour les tâches Container_Scan (ID:18) et Custom_Container_Scan (ID:19)

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0
```

```
ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes

QueueScanTasks=No
```

Vous pouvez également utiliser les paramètres de ce fichier de configuration pour la tâche Analyse personnalisée du conteneur.

Paramètres par défaut de la tâche Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes
```

```
TelemetrySource=Default
```

Paramètres par défaut de la tâche Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Paramètres par défaut de la tâche Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche KATAEDR (ID:24)

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]
```

```
MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Paramètres par défaut pour la tâche Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Paramètres par défaut de la tâche Standalone_Sandbox (ID:29)

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes
```

```
ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

Paramètres par défaut de la tâche KATANDR (ID:31)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

Paramètres par défaut de la tâche KUMA (ID:33)

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

Paramètres par défaut de la tâche Protection contre les menaces par emails (ID : 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible

ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt
```

```
[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi

[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

Paramètres par défaut de la tâche Protection BadUSB (ID:37)

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

Paramètres par défaut de la tâche KATANDR (ID:31)

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
```

```
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

Annexe 2. Configuration de la collaboration avec Kaspersky Antivirus for Linux Mail Server

Pour configurer la compatibilité entre l'application Kaspersky Endpoint Security et Kaspersky Anti-Virus for Linux Mail Server :

1. Enregistrez les paramètres de la tâche Protection contre les fichiers malicieux dans le fichier de configuration à l'aide de la commande suivante :

   `kesl-control --get-settings 1 --file <chemin d'accès complet au fichier>`

2. Ouvrez le fichier de configuration créé afin d'en modifier le contenu.

3. Ajoutez la section suivante dans le fichier créé :

   `[ExcludedFromScanScope.item_<numéro d'élément>]`

   `Path=/var/opt/kaspersky/klms`

4. Répéter la section indiquée ci-dessus pour tous les agents de messagerie intégrés à Kaspersky Anti-Virus for Linux Mail Server.

5. Pour exclure le répertoire temporaire des filtres et des services de Kaspersky Anti-Virus for Linux Mail Server de l'analyse, ajoutez la section suivante dans le fichier créé la section :

   `[ExcludedFromScanScope.item_<numéro d'élément>]`

   `Path=/tmp/klmstmp`

6. Enregistrez les modifications dans le fichier de configuration.

7. Importez les paramètres du fichier de configuration dans la tâche Protection contre les fichiers malicieux à l'aide de la commande suivante :

   `kesl-control --set-settings 1 --file <chemin d'accès complet au fichier>`

Annexe 3. Paramètres d'interaction avec les services externes

Kaspersky Endpoint Security utilise les paramètres réseau et de chiffrement suivants pour communiquer avec les services externes.

Paramètres d'interaction avec les services externes

Adresse réseau du service et protocole	Description
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocole : `HTTPS` Port : `443`	Activation de l'application.

Adresse réseau du service et protocole	Description
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com Protocole : HTTPS Port : 443	Mise à jour des bases et des modules de l'application.

Adresse réseau du service et protocole	Description
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com Protocole : HTTP Port : 80	Mise à jour des bases et des modules de l'application.
downloads.upd.kaspersky.com Protocole : HTTPS Port : 443	• Mise à jour des bases et des modules de l'application. • Vérification de l'accès aux serveurs de Kaspersky. Si l'accès aux serveurs via le DNS système échoue, l'application utilisera le DNS public. Ceci est nécessaire pour la mise à jour des bases de l'application et maintenir le niveau de sécurité de l'appareil. L'application utilisera les DNS publics suivants par ordre d'apparition : 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Les demandes de l'application peuvent contenir des adresses de domaine et l'adresse IP externe de l'utilisateur, car l'application établit une connexion TCP/UDP avec le serveur DNS. Ces données sont nécessaires, par exemple, pour l'analyse du certificat d'une ressource Internet lors de l'accès via HTTPS. Si l'application utilise un serveur DNS public, les règles de traitement des données sont régies par la Politique de confidentialité de ce service.
ds.kaspersky.com Protocole : HTTPS Port : 443	Utilisation de Kaspersky Security Network.

Adresse réseau du service et protocole	Description
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Protocole : KSN Port : 443, 1443	Utilisation de Kaspersky Security Network.
click.kaspersky.com Protocole : HTTPS Port : 443	Suivez les liens depuis l'interface.
crl.kaspersky.com ocsp.kaspersky.com Protocole : HTTP Port : 80	Infrastructure à clés publiques (ICP). Ces serveurs (crl.kaspersky.com) font partie de l'infrastructure à clé publique (PKI) et sont nécessaires pour vérifier la validité des certificats de signature numérique de Kaspersky. Le serveur CRL fournit une liste des certificats révoqués. Le service OCSP vous permet de consulter en temps réel l'état d'un certificat spécifique. Le fonctionnement de ces modules garantit la sécurité des interactions avec les certificats numériques et la protection contre les attaques potentielles.

Annexe 4. Extensions de fichiers pour l'analyse rapide des disques amovibles

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64 Ko ;

exe : fichier exécutable, archive autoextractible ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase™, Clipper ou Microsoft Visual FoxPro®, programme de la suite WAVmaker ;

bin : fichier binaire ;

bat : fichier de paquet ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compressée ;

dll : bibliothèque dynamique ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme qui fonctionne en mode de partage du temps ;

drv : pilote d'un appareil quelconque ;

vxd : pilote d'un appareil virtuel Microsoft Windows ;

pif : fichier contenant des informations sur un logiciel ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registre de Microsoft Windows ;

ini : fichier de configuration qui contient les données des paramètres pour Microsoft Windows, Windows NT et pour certaines applications ;

cla : classe Java ;

vbs : script Visual Basic® ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer® ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

msg : email de Microsoft Mail ;

plg : email ;

mbx : email Microsoft Office Outlook enregistré ;

doc* : documents Microsoft Office Word, par exemple, doc : document Microsoft Office Word, docx : document Microsoft Office Word 2007 compatible avec XML, docm : document Microsoft Office Word 2007 compatible avec les macros ;

dot* : modèles de document Microsoft Office Word, par exemple, dot : modèle de document Microsoft Office Word, dotx : modèle de document Microsoft Office Word 2007, dotm : modèle de document Microsoft Office Word 2007 compatible avec les macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Windows Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD® ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave® Flash ;

jpg, jpeg : fichier graphique de conservation de données compressées ;

emf : fichier au format Enhanced Metafile ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutables Microsoft Office Word ;

xl* : les documents et les fichiers de Microsoft Office Excel, tels que, xla : extension Microsoft Excel, xlc : schéma, xlt : modèle des documents, xlsx : feuille de calcul Microsoft Office Excel 2007, xltm : feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, xlsb : feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), xltx : modèle Microsoft Office Excel 2007, xlsm : modèle Microsoft Office Excel 2007 compatible avec les macros, xlam : modèle externe Microsoft Office Excel 2007 compatible avec les macros ;

pp* : les documents et les fichiers de Microsoft Office PowerPoint®, tels que, pps : diaporama Microsoft Office PowerPoint, ppt : présentation, pptx : présentation Microsoft Office PowerPoint 2007, pptm : présentation Microsoft Office PowerPoint 2007 compatible avec les macros, potx : modèle de présentation Microsoft Office PowerPoint 2007, potm : modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, ppsx : diaporama Microsoft Office PowerPoint 2007, ppsm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, ppam : module externe Microsoft Office PowerPoint 2007 compatible avec les macros ;

md* : documents et fichiers de Microsoft Office Access® tels que, mda : groupe de travail de Microsoft Office Access, mdb : base de données ;

sldx : diaporama Microsoft Office PowerPoint 2007 ;

sldm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros ;

thmx : thème Microsoft Office 2007.

Annexe 5. Variables dans les modèles de messages

Les modules Contrôle des appareils et Contrôle Internet permettent de configurer des modèles de messages que Kaspersky Endpoint Security affiche à l'intention d'un utilisateur qui tente d'accéder à un appareil, une application ou une ressource bloquée, ou qui tente d'effectuer une action potentiellement dangereuse.

Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.

Variables dans les modèles de messages du Contrôle des appareils

Vous pouvez utiliser les variables suivantes dans les modèles de messages utilisateur ou administrateur :

- **Utilisateur** – `%USER_NAME%`.

  Nom du compte utilisateur actuel de l'ordinateur sur lequel le message a été généré, dans le format `<device name>\<user alias>` (par exemple, `DESKTOP-123\John.Smith`).

- **Ordinateur** – `%COMPUTER_NAME%`.

  Nom de l'ordinateur sur lequel un appareil a été bloqué.

- **Nom de la règle** – `%RULE%`.

  Nom de la règle qui a bloqué l'appareil.

- **Date de déclenchement de la règle** – `%DATE%`.

  Date à laquelle l'appareil a été bloqué au format JJ.MM.AAAA.

- **Heure de déclenchement de la règle** – `%TIME%`.

  Heure à laquelle l'appareil a été bloqué au format HH:MM.

- **Nom de l'appareil** – `%DEVICE_NAME%`.

  Nom de l'appareil bloqué.

- **Type d'appareil** – `%DEVICE_TYPE%`.

  Type de l'appareil bloqué (par exemple, imprimantes, disques amovibles, lecteurs de CD/DVD).

- **Modèle de l'appareil** – `%DEVICE_VIDPID%`.

  Modèle de l'appareil bloqué (par exemple, VID_1234&PID_5678).

- **Identifiant d'appareil** – `%DEVICE_ID%`.

  Identifiant de l'appareil bloqué (par exemple, `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`).

- **Opérations de l'appareil** – `%OPERATION%`.

  Type d'opération interdite avec l'appareil.

Variables dans les modèles de message du Contrôle Internet

Vous pouvez utiliser les variables suivantes dans les modèles de messages utilisateur ou administrateur :

- **Utilisateur** – %USER_NAME%.

  Nom du compte utilisateur actuel de l'ordinateur sur lequel le message a été généré, dans le format <device name>\<user alias> (par exemple, DESKTOP-123\John.Smith).

- **Adresse de la ressource Internet** – %CANONIC_REQUEST_URL%.

  Adresse de la ressource Internet bloquée.

- **Nom de la règle** – %RULE%.

  Nom de la règle qui a bloqué la ressource Internet.

- **Adresse pour les messages** – %COMPLAIN_EMAIL%.

  Adresse email pour les commentaires concernant les blocs de ressources Internet. En cliquant sur l'adresse email, une fenêtre s'ouvre dans laquelle l'utilisateur peut écrire un message à l'administrateur.

- **Nom de catégorie de contenu** – %CONTENT_CATEGORY_LIST%.

  Catégorie de site Internet à laquelle appartient la ressource bloquée (par exemple, *Systèmes de paiement*).

- **Nom de catégorie du type de données** – %TYPE_CATEGORY_LIST%.

  Catégorie de type de données sur la ressource Internet bloquée (par exemple, *Fichiers graphiques*).

- **Lien vers la ressource Internet demandée** – %CONTINUE_PAGE%.

  Lien vers la page Internet demandée (par exemple, http://www.example.com/pagename.html).

- **Lien vers le site** – %CONTINUE_SITE%.

  Lien vers le site Internet qui contient la page Internet demandée (par exemple, http://www.example.com/).

- **Lien d'accès aux domaines** – %CONTINUE_DOMAIN%.

  Lien cliquable permettant d'accéder à toutes les pages Internet existantes du nom de domaine. Par exemple, si l'adresse de la page Internet bloquée est http://www.example.com, la variable %CONTINUE_DOMAIN% est remplacée par le lien http://*.example.com. Ce lien permet d'accéder à toutes les adresses Internet du nom de domaine de base http://www.example.com/, y compris les sous-domaines, par exemple, http://start.example.com/* ou http://domain.domain.example.com/*, où le caractère * représente n'importe quelle séquence de caractères (y compris une chaîne vide).

Annexe 6. Événements relatifs aux applications

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'achèvement de chaque tâche d'analyse des logiciels malveillants, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans le journal des événements de Kaspersky Security Center et dans le journal des événements du système d'exploitation (syslog).

Critique

Violation de l'intégrité du système

État	ⓘ
Module	Contrôle de l'intégrité du système
ID de l'événement Linux	0
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_FIM_ALARM
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Démarrage de l'application refusé

État	ⓘ
Module	Contrôle des applications
ID de l'événement Linux	122
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet malveillant détecté (bases de données locales)

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Détection comportementale Protection contre les Exploits Sandbox
ID de l'événement Linux	6
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Limite d'événements du Contrôle de l'intégrité du système dépassée

État	ⓘ
Module	Contrôle de l'intégrité du système
ID de l'événement Linux	70
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_FIM_ALARM_OVERFLOW
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Opération avec l'appareil interdite

État	ⓘ
Module	Contrôle des appareils
ID de l'événement Linux	94
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Attaque réseau détectée

État	⊗
Module	Protection contre les menaces réseau
ID de l'événement Linux	102
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès refusé (bases de données locales)

État	⊗
Module	Contrôle Internet
ID de l'événement Linux	190
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Avertissement

Désinfection impossible

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails
ID de l'événement Linux	10
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Avertissement relatif au contenu indésirable (bases de données locales)

État	⚠
Module	Contrôle Internet
ID de l'événement Linux	192
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Message à l'administrateur concernant le blocage de l'accès à une page Web

État	⚠
Module	Contrôle Internet
ID de l'événement Linux	196

Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Messages d'information

Objet désinfecté

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails
ID de l'événement Linux	9
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet supprimé

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails
ID de l'événement Linux	8
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Démarrage de l'application autorisé

État	ⓘ
Module	Contrôle des applications
ID de l'événement Linux	120
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCHED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center	non configuré

Démarrage de l'application autorisé en mode test

État	ⓘ
Module	Contrôle des applications
ID de l'événement Linux	121
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Démarrage de l'application refusé en mode test

État	ⓘ
Module	Contrôle des applications
ID de l'événement Linux	123
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Appareil connecté

État	ⓘ
Module	Contrôle des appareils
ID de l'événement Linux	90
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Appareil déconnecté

État	ⓘ
Module	Contrôle des appareils
ID de l'événement Linux	91
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Journal (syslog) (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Annexe 7. Codes de retour

Codes de retour de l'Assistant de configuration initiale

0 – Installation terminée avec succès.

Erreurs critiques

1 – Erreur inconnue (toutes les autres erreurs critiques, à l'exception de celles répertoriées ci-dessous, par exemple : erreurs système, mémoire insuffisante, erreur d'ouverture de fichier, etc.).

2 – Le fichier de configuration initiale contient des paramètres non valides.

3 – Échec de l'installation ou de la mise à jour de l'application.

4 – Impossible de supprimer l'application.

5 – Impossible de démarrer l'application. Raison possible : les droits d'accès ne sont pas correctement configurés. Vérifiez que seul le compte root dispose du droit d'écriture dans les répertoires suivants : /, /opt, /opt/kaspersky, /var, /var/opt, /var/opt/kaspersky, /usr et /usr/lib64.

6 – Les actions nécessaires n'ont pas été effectuées avant l'installation.

7 – Échec de la mise à jour de l'application. L'installation d'une version antérieure de l'application n'est pas prise en charge.

8 – Échec de la suppression des utilisateurs des groupes privilégiés.

9 – Échec de la création d'un MachineID unique pour l'installation de l'application.

10 – Échec du démarrage ou du redémarrage de l'application.

11 – Les conditions générales du Contrat de licence utilisateur final (EULA) et de la Politique de confidentialité n'ont pas été acceptées.

12 – L'application ne peut pas être utilisée simultanément en mode Light Agent et en mode EDR Agent.

13 – Le paquet astra-digsig-oldkeys pour le mode d'environnement logiciel fermé dans Astra Linux est introuvable.

14 – La configuration initiale a déjà été lancée.

15 – Le module Light Agent for Linux, installé dans le cadre de la solution Kaspersky Security for Virtualization 5.2 Light Agent, doit être supprimé.

16 – L'Agent d'administration de Kaspersky Security Center doit être installé.

17 – Échec du lancement de l'Assistant de configuration initiale en raison d'un processus de l'application déjà en cours d'exécution.

18 – fanotify n'est pas pris en charge. Échec de la compilation d'un module de noyau pour la Protection contre les fichiers malicieux.

19 – Les droits d'administrateur sont requis pour l'installation.

20 – Le service de l'application n'a pas été démarré.

21 – La mise à jour de l'application a été annulée.

22 – L'intégration de l'application en mode EDR Agent ou en mode Light Agent avec Kaspersky Endpoint Detection and Response Expert (cloud) n'est pas prise en charge.

Avertissements

71 – Plusieurs avertissements lors de l'installation. Consultez le journal d'installation pour plus de détails.

72 – Échec de la mise à jour des bases de données de l'application.

75 – Le redémarrage du système d'exploitation est requis.

76 – Échec de l'application des paramètres KSN ou les conditions générales de la Déclaration KSN n'ont pas été acceptées.

77 – Échec du démarrage d'un module de noyau mis à jour.

79 – Échec de l'installation ou de la mise à jour du paquet de l'interface graphique de l'application.

80 – Échec du téléchargement des bases de données de l'application.

81 – L'activation de l'application s'est terminée par une erreur en raison de problèmes réseau.

82 – L'application est administrée par une stratégie.

83 – L'interface graphique de l'application n'a pas été lancée.

84 – Échec de l'attribution du rôle d'administrateur. L'utilisateur spécifié est introuvable.

85 – Le paquet de l'application n'a pu être installé ou mis à jour qu'en mode d'ignorance des erreurs du gestionnaire de paquets.

86 – Échec de la suppression du paquet de l'interface graphique de l'application.

87 – Le paquet de l'application n'a pu être supprimé qu'en mode d'ignorance des erreurs du gestionnaire de paquets.

88 – Échec de l'attribution du rôle d'administrateur à l'utilisateur.

89 – Clé de licence non valide.

90 – Échec de la définition d'une programmation pour la tâche de mise à jour.

Codes de retour de l'utilitaire de ligne de commande kesl-control

0 – Commande/tâche exécutée avec succès.

1 – Erreur générale dans la syntaxe de la commande.

2 – Erreur dans les paramètres de l'application transmis.

64 : l'application Kaspersky Endpoint Security n'est pas lancée ;

66 – Les bases de données de l'application ne sont pas chargées (ce code est utilisé uniquement par la commande `kesl-control --app-info`).

67 – L'activation de l'application s'est terminée par une erreur en raison de problèmes réseau.

68 – Impossible d'exécuter la commande car l'application est administrée par une stratégie.

69 – L'application se trouve dans l'infrastructure Amazon Paid Ami.

70 – Tentative de lancement d'une tâche déjà en cours d'exécution, de suppression d'une tâche en cours d'exécution, de modification des paramètres d'une tâche en cours d'exécution, d'arrêt d'une tâche arrêtée, de suspension d'une tâche suspendue ou de reprise d'une tâche en cours d'exécution.

71 : rejet des dispositions de la Déclaration de Kaspersky Security Network ;

72 – Des menaces ont été détectées lors de l'exécution de la tâche Analyse personnalisée ou Analyse personnalisée du conteneur.

73 – Tentative de définition de paramètres de la tâche Contrôle des applications ayant un impact sur le fonctionnement de l'application, sans les confirmer à l'aide de l'option `--accept`.

74 : la mise à jour requiert le relancement de l'application Kaspersky Endpoint Security ;

75 – L'appareil doit être redémarré.

76 – Connexion interdite, car seuls les utilisateurs disposant de droits root doivent disposer d'un accès en écriture au chemin spécifié.

77 – La clé de licence spécifiée est déjà utilisée sur l'appareil.

78 – Impossible d'exécuter la commande/tâche car l'application est utilisée en mode Light Agent.

79 – Impossible d'exécuter la commande car l'application est utilisée en mode standard.

80 – L'opération de téléchargement de la mise à jour a échoué en raison de problèmes réseau.

81 – Le module n'est pas pris en charge dans la version du système d'exploitation installée sur l'appareil.

128 – Erreur inconnue.

65 : toutes les autres erreurs.

Annexe 8. Préparation d'une archive contenant les bases de données de l'application

Lors de la création manuelle d'un paquet d'installation de Kaspersky Endpoint Security, vous pouvez y ajouter des bases de données de l'application téléchargées précédemment. Si un paquet d'installation avec des bases de données intégrées est utilisé pour l'installation, l'application est installée avec des bases de données fonctionnelles ; il n'est pas nécessaire de mettre à jour les bases de données immédiatement après l'installation.

L'ajout des bases de données de l'application au paquet d'installation augmente la taille de ce dernier.

Vous aurez besoin d'un ensemble distinct de bases de données de l'application pour chaque combinaison d'architecture et de nombre de bits du système d'exploitation de vos appareils protégés. Vous pouvez ajouter au paquet d'installation une archive contenant un ou plusieurs ensembles de bases de données de l'application. Pour préparer chaque ensemble de bases de données de l'application, vous avez besoin d'une instance de l'application Kaspersky Endpoint Security déjà installée sur un appareil doté d'un système d'exploitation dont l'architecture et le nombre de bits correspondent.

Pour préparer une archive contenant les bases de données :

1. Installez Kaspersky Endpoint Security sur l'appareil et effectuez sa configuration initiale à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

2. Mettez à jour les bases de données de l'application sur l'appareil. Vous pouvez mettre à jour les bases de données lors de la configuration initiale de l'application ou après l'installation en exécutant une tâche *Update* sur la ligne de commande ou une tâche *Update* dans Kaspersky Security Center.

3. Créez un répertoire pour les bases de données en fonction de l'architecture et du nombre de bits du système d'exploitation de l'appareil protégé :

   - x86_64 si l'application est installée sur un système d'exploitation 64 bits
   - i386 si l'application est installée sur un système d'exploitation 32 bits
   - arm64 si l'application est installée sur un système d'exploitation 64 bits pour l'architecture Arm
   - e2k si l'application est installée sur un système d'exploitation 64 bits pour l'architecture Elbrus

4. Copiez le contenu du répertoire /var/opt/kaspersky/kesl/private/updates dans le répertoire de bases de données créé.

5. Ajoutez le répertoire de bases de données créé à l'archive kesl-bases.tgz.

   Si vous souhaitez créer un paquet d'installation pour l'installation sur plusieurs systèmes d'exploitation avec différentes architectures et différents nombres de bits, vous devez préparer plusieurs répertoires contenant les bases de données et les ajouter tous à l'archive kesl-bases.tgz.

Par défaut, la tâche de mise à jour des bases de données est lancée après l'installation de l'application Kaspersky Endpoint Security. Si vous installez une application à partir d'un paquet d'installation avec des bases de données intégrées, désactivez la tâche de mise à jour des bases de données après l'installation de l'application. Vous pouvez configurer ce paramètre dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini (`UPDATE_EXECUTE=No`).

Annexe 9. Exigences pour les fichiers IOC

Lorsque vous créez des tâches d'analyse IOC, tenez compte des exigences et des limites suivantes relatives aux fichiers IOC :

- L'application prend en charge les fichiers IOC avec l'extension .IOC et .XML du standard ouvert pour décrire les indicateurs de compromission OpenIOC versions 1.0 et 1.1.
- Les erreurs sémantiques et les termes et tags IOC non pris en charge dans les fichiers IOC ne provoquent pas d'erreurs d'exécution de la tâche. Dans ces sections des fichiers IOC, l'application enregistre l'absence de concordance.
- Les identifiants de tous les fichiers IOC utilisés dans une seule tâche d'analyse IOC doivent être uniques. S'il y a des fichiers IOC avec le même identifiant, cela peut affecter les résultats de l'exécution de la tâche.
- Il est recommandé de créer un fichier IOC pour chaque menace. Cela facilite la lecture des résultats de la tâche *Analyse IOC*.

Le fichier, qui peut être téléchargé à partir du lien ci-dessous, contient un tableau avec une liste complète des termes IOC de la norme OpenIOC.

TÉLÉCHARGER LE FICHIER IOC TERMS.XLSX

Les fonctionnalités et limitations de la prise en charge des applications pour la norme OpenIOC sont présentées dans le tableau ci-dessous.

Fonctionnalités et limitations de la prise en charge des versions 1.0 et 1.1 du standard OpenIOC.

Conditions prises en charge	OpenIOC 1.0 : • `is` • `isnot` (à titre d'exclusion parmi les nombreux) • `contains` • `containsnot` (à titre d'exclusion parmi les nombreux) OpenIOC 1.1 : • `is` • `contains` • `starts-with` • `ends-with` • `matches` • `greater-than` • `less-than`
Attributs des conditions prises en charge	OpenIOC 1.1 : • `preserve-case` • `negate`
Opérateurs pris en charge	`AND` `OR`
Types de données pris en charge	`"date"` : date (conditions applicables : `is`, `greater-than`, `less-than`) `"int"` : nombre entier (conditions applicables : `is`, `greater-than`, `less-than`) `"string"` : ligne (conditions applicables : `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"` : durée en secondes (conditions applicables : `is`, `greater-than`, `less-than`)

Caractéristiques de l'interprétation des types de données	Les types de données `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` sont interprétés comme une ligne (string).
	L'application prend en charge l'interprétation du paramètre `Content` pour les types de données `int` et `date`, spécifiés sous forme d'intervalles :
	• OpenIOC 1.0 :
	Utilisation de l'opérateur `TO` dans le champ `Content` :
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1 :
	◦ Utilisation de conditions `greater-than` et `less-than`
	◦ Utilisation de l'opérateur `TO` dans le champ `Content`
	
	L'application prend en charge l'interprétation des types de données `date` et `duration` si les indicateurs sont spécifiés au format `ISO 8601, Zulu time zone, UTC`.

Mentions légales

À propos des données

Cette section contient des informations sur les données que Kaspersky Endpoint Security peut enregistrer sur l'appareil et transférer automatiquement à Kaspersky au cours de son fonctionnement.

Kaspersky protège toutes les informations ainsi reçues conformément à la loi et aux règles applicables de Kaspersky Les données sont transmises via des canaux de communication chiffrés.

Pour en savoir plus sur le traitement, le stockage et la destruction des informations obtenues pendant l'utilisation de l'application et transmises à Kaspersky, veuillez lire le Contrat de licence utilisateur final, la Déclaration de Kaspersky Security Network et la Politique de confidentialité sur le site de Kaspersky. Les fichiers license.<identifiant de la langue> et ksn_license.<identifiant de la langue> contiennent le Contrat de licence utilisateur final et la Déclaration de Kaspersky Security Network et font partie du kit de distribution de l'application.

Données fournies lors de l'utilisation d'un code d'activation

Si l'application Kaspersky Endpoint Security est utilisée en mode standard ou en mode EDR Agent et est activée à l'aide d'un code d'activation, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes afin de vérifier la légitimité de l'utilisation de l'application et d'obtenir des informations statistiques sur la distribution et l'utilisation de l'application :

- type, version et localisation de l'application installée ;
- versions des mises à jour installées de l'application ;
- identifiant de l'appareil et identifiant de l'installation de l'application sur l'appareil ;
- code d'activation utilisé pour activer l'application ;
- ID de la licence actuelle ;
- date et heure de création de la clé de licence de l'application ;
- date et heure sur l'appareil de l'utilisateur ;
- date et heure d'expiration de la durée de validité de la licence de l'application ;
- type, version et nombre de bits du système d'exploitation.

Données fournies lors du téléchargement des mises à jour depuis les serveurs de mise à jour de Kaspersky

Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode EDR Agent et que vous utilisez les serveurs de mise à jour de Kaspersky pour télécharger les mises à jour, dans le but d'améliorer l'efficacité de la procédure de mise à jour et de fournir des informations statistiques sur la distribution et l'utilisation de l'application, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes :

- ID de l'application provenant de la licence ;
- version complète de l'application ;
- ID de licence de l'application ;
- type de licence de l'application utilisé ;
- ID de l'installation de l'application (PCID) ;
- ID du démarrage de la mise à jour de l'application ;
- adresse Internet en cours de traitement.

Données transférées lors de l'utilisation de l'application en mode Light Agent

Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent dans le cadre de Kaspersky Security for Virtualization Light Agent, elle enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles, et les envoie aux autres modules de la solution pendant le fonctionnement de l'application.

- Pour l'activer, l'application Kaspersky Endpoint Security transfère les données suivantes au Serveur de protection : la période de validité de la confirmation de l'état de la clé de licence, l'identifiant (BIOS ID) de la machine virtuelle protégée, les informations sur la licence requise par le Light Agent pour fonctionner.
- Pour mettre à jour les bases de données du Light Agent, l'application Kaspersky Endpoint Security transfère les données suivantes au Serveur de protection : identifiant du logiciel obtenu grâce à la licence ; version complète du logiciel ; identifiant de licence de logiciel ; identifiant d'installation du logiciel (PCID) ; adresse Internet traitée ; type de licence installée ; identifiant de lancement d'une mise à jour.
- Pour assurer la protection et pendant les tâches d'analyse, l'application Kaspersky Endpoint Security transfère au Serveur de protection les informations nécessaires à l'analyse des objets. Cela inclut les noms de fichiers et leurs chemins d'accès dans le système de fichiers, les hachages de fichiers, les adresses Web, ainsi que les objets analysés ou leurs fragments.
- Dans une infrastructure gérée par VMware vCenter Server et VMware NSX Manager, l'application Kaspersky Endpoint Security peut transmettre au Serveur d'intégration des informations sur les tags de sécurité attribuées à une machine virtuelle protégée lorsque des virus, des logiciels malveillants et des activités typiques d'attaques réseau sont détectés. Cela inclut le transfert des identifiants des machines virtuelles protégées.

- Pour obtenir les informations utilisées lors de la sélection d'une SVM pour la connexion, l'application Kaspersky Endpoint Security transmet l'identifiant de la machine virtuelle protégée au Serveur d'intégration et au Serveur de protection.

- Lors de l'utilisation de la solution Kaspersky Security for Virtual Environments Light Agent en mode multi-tenant, les informations nécessaires à la génération des rapports sur la protection des locataires peuvent être transférées de l'application Kaspersky Endpoint Security vers le Serveur de protection. Peuvent être transmis : l'identifiant de la machine virtuelle protégée ; type et version du système d'exploitation invité sur la machine virtuelle protégée ; périodes pendant lesquelles l'application Kaspersky Endpoint Security était connectée à la SVM.

- Pour obtenir des statistiques, l'application Kaspersky Endpoint Security transmet les informations suivantes au Serveur de protection : des informations sur la version du système d'exploitation de la machine virtuelle protégée ; localisation de l'application Kaspersky Endpoint Security ; noms des modules actifs de l'application Kaspersky Endpoint Security ; identifiant (BIOS ID) de la machine virtuelle protégée.

Les informations spécifiées, en plus des informations nécessaires pour effectuer la vérification de l'objet et des informations utilisées lors de la sélection d'un SVM, sont transmises sur des canaux de données cryptés. La connexion entre l'application Kaspersky Endpoint Security et les Serveurs de protection n'est pas sécurisée par défaut. Vous pouvez activer le chiffrement du canal de transmission des données entre les Light Agents et les Serveurs de protection dans les paramètres de l'application Kaspersky Endpoint Security.

Données transmises à l'application Kaspersky Security Center

Pendant son fonctionnement, l'application Kaspersky Endpoint Security enregistre des informations et les transmet à l'application Kaspersky Security Center. Ces informations peuvent contenir des données personnelles et confidentielles :

- Informations relatives aux bases que l'application utilise :
  - liste des catégories de bases indispensables à l'application ;
  - date et heure de la publication et du chargement des bases que l'application utilise ;
  - date d'édition des mises à jour des bases de l'application téléchargées ;
  - date et heure de la dernière publication des bases de l'application ;
  - le nombre d'enregistrements dans les bases de données d'application actuellement utilisées.
- Informations sur la licence d'utilisation de l'application :
  - numéro de série et type de la licence ;
  - durée de validité de la licence en jours ;
  - nombre d'appareils couverts par la licence ;
  - date de début et de fin de validité de la licence ;
  - état de la clé de licence ;
  - date et heure de la dernière synchronisation réussie avec les serveurs d'activation, si l'application a été activée à l'aide d'un code d'activation ;

- ID de l'application dont la licence est prévue pour l'activation ;
- fonctionnalités disponibles sous la licence ;
- nom de l'organisation à laquelle la licence a été octroyée ;
- informations complémentaires en cas d'utilisation de l'application selon un abonnement (empreinte de l'abonnement, date de fin d'abonnement et nombre de jours disponibles pour renouveler l'abonnement, adresse Internet du fournisseur de l'abonnement, état actuel et raison du passage à cet état), date et heure d'activation de l'application sur l'appareil ;
- Date et heure de fin de validité de la licence sur l'appareil

- Informations relatives aux mises à jour de l'application :
  - liste des mises à jour à installer ou à supprimer ;
  - date d'édition de la mise à jour et présence de l'état *Critique* ;
  - nom, version et brève description de la mise à jour ;
  - lien vers l'article contenant la description complète de la mise à jour ;
  - ID et texte du Contrat de licence utilisateur final et de la Politique de confidentialité pour la mise à jour de l'application ;
  - ID et texte de la Déclaration de Kaspersky Security Network pour la mise à jour de l'application ;
  - indice de la possibilité de supprimer la mise à jour ;
  - version de la stratégie et du plug-in d'administration de l'application ;
  - adresse Internet pour le téléchargement du plug-in d'administration de l'application ;
  - nom des mises à jour de l'application installées, versions et dates d'installation ;
  - code et description de l'erreur si l'installation ou la suppression de la mise à jour s'est soldée sur une erreur ;
  - indice et raison de la nécessité de redémarrer le appareils ou l'application à cause de la mise à jour de l'application
- Acceptation ou refus des conditions de la Déclaration de Kaspersky Security Network, du Contrat de licence utilisateur final et de la Politique de confidentialité.
- Liste des tags attribués aux appareils.
- Liste des états des appareils et raison de leur attribution.
- État général de l'application et état de tous ses modules ; informations sur la conformité à la stratégie, état de protection en temps réel de l'appareil, état de stabilité de l'application, informations sur l'arrêt de l'application.
- Date et heure de la dernière analyse de l'appareil ; nombre d'objets analysés ; nombre d'objets malveillants détectés ; nombres d'objets bloqués, supprimés ou désinfectés ; nombre d'objets dont la réparation était impossible ; nombre d'erreurs d'analyse ; nombre d'attaques de réseau détectées.
- Données relatives aux valeurs actuelles des paramètres de l'application.

- État actuel et résultats d'exécution des tâches de groupe et des tâches locales, ainsi que paramètres des tâches.
- Informations relatives aux appareils externes connectés à l'appareil client (ID, nom, type, fabricant, description, numéro de série et VID/PID).
- Informations relatives aux copies de sauvegarde placés dans la sauvegarde (nom, chemin d'accès, taille et type de l'objet, description de l'objet, nom de la menace détectée, version des bases de l'application qui ont détecté la menace, date et heure de l'enregistrement de l'objet dans la sauvegarde, action réalisée sur l'objet dans la sauvegarde (suppression, restauration)) ainsi que les fichiers à la demande de l'administrateur.
- Informations relatives au fonctionnement de chaque module de l'application ou à l'exécution de chaque tâche sous la forme d'un événement :
  - date et heure de l'événement ;
  - nom et type de l'événement ;
  - gravité de l'événement ;
  - nom de la tâche ou du module de l'application au cours du fonctionnement duquel s'est produit l'événement ;
  - informations relatives à l'application qui a provoqué l'événement : nom de l'application, chemin d'accès au fichier sur le disque, ID de processus, valeurs des paramètres en cas de publication de l'événement du lancement ou de modification des paramètres de fonctionnement de l'application ;
  - ID de l'utilisateur
  - nom de l'initiateur (planificateur de tâche, application, Kaspersky Security Center ou nom d'utilisateur) dont l'action a provoqué l'événement ;
  - nom et identificateur de l'utilisateur qui a initialisé l'accès au fichier ;
  - résultat du traitement de l'objet ou de l'action (description, type, nom, niveau de danger et précision, nom du fichier et type d'opération sur l'appareil, décision de l'application suite à cette opération) ;
  - informations relatives à l'objet (nom et type d'objet, chemin d'accès à l'objet sur le disque, version de l'objet, taille, informations relatives à l'action exécutée, description de la raison de l'événement, description de la raison du non-traitement et du laisser-passer de l'objet) ;
  - des informations sur l'appareil (nom du fabricant, nom de l'appareil, chemin d'accès, type d'appareil, type de bus, identifiant, VID/PID, attribut de l'appareil système, nom de la planification des règles d'accès à l'appareil) ;
  - informations relatives au blocage et au déblocage de l'appareil ; informations relatives aux connexions bloquées (nom, description, nom de l'appareil, protocole, adresse distante et port, adresse locale et port, règles pour les paquets, actions) ;
  - informations relatives à l'adresse Internet sollicitée ;
  - informations relatives aux objets détectés ;
  - type de détection, méthode et identifiant ;
  - informations relatives à l'action exécutée ;

- informations relatives aux bases de l'application (date d'édition des mises à jour des bases téléchargées, informations relatives à l'application des bases, erreurs d'application des bases, informations relatives à l'annulation des mises à jour des bases installées) ;
- informations relatives à la détection d'un chiffrement malveillant (nom du chiffreur ; nom de l'appareil sur lequel le chiffrement malveillant a été détecté, informations relatives au blocage ou au déblocage de l'appareil) ;
- paramètres de l'application et paramètres de réseau ;
- informations relatives à la règle du Contrôle des applications appliquée (nom et type) et le résultat de son application ;
- informations relatives aux conteneurs et aux images de conteneur (noms des conteneurs ou des images de conteneurs, chemin d'accès aux conteneurs ou aux images de conteneur, adresse Internet du référentiel) ;
- informations relatives aux connexions actives et bloquées (nom, description et type) ;
- informations relatives au blocage et au déblocage de l'accès aux appareils douteux
- des informations sur l'utilisation du KSN (état de connexion au KSN, infrastructure du KSN, identifiant de la déclaration KSN en mode avancé, acceptation de la Déclaration KSN en mode avancé, identifiant de la Déclaration KSN, acceptation de la Déclaration KSN) ;
- informations relatives aux certificats (nom de domaine, nom du sujet, nom de l'émetteur, date d'expiration, état du certificat, type de certificat, heure d'ajout du certificat, date d'émission, numéro de série, empreinte SHA256) ;
- informations sur les systèmes externes faisant partie des solutions logicielles de l'entreprise (adresse du serveur d'intégration) ;
- des informations sur l'activation et la désactivation de l'isolement du réseau pour l'appareil ;
- des informations sur le travail en mode Light Agent : nom du modèle de machine virtuelle, adresse du Serveur d'intégration ;
- le nom de l'appareil pour lequel l'isolation réseau est activée ou désactivée ;
- statistiques d'exécution des tâches d'analyse : nombre d'objets analysés ; nombre de menaces trouvées ; nombre d'objets infectés ; nombre d'objets éventuellement infectés ; nombre d'objets désinfectés ; nombre d'objets ajoutés à la sauvegarde ; nombre d'objets supprimés ; nombre d'objets non réparés ; nombre d'erreurs de vérification ; nombre d'objets protégés par un mot de passe ; nombre d'objets manqués ; nombre de conteneurs et d'images vérifiés ;
- informations sur la version du module EDR Optimum utilisé dans l'application ;
- informations sur les chaînes de développement des menaces : nom de la liste réseau des chaînes de développement des menaces, identifiant de la chaîne de développement des menaces.

- Informations relatives au fonction de la tâche de vérification de l'intégrité du système (nom, type, chemin) et informations relatives à la capture de l'état du système.
- Informations relatives à l'activité réseau, aux règles pour les paquets et aux attaques réseau.

- Informations relatives au rôle de l'utilisateur :
  - nom et identificateur de l'utilisateur qui a lancé la modification du rôle utilisateur ;
  - rôle utilisateur ;
  - nom d'utilisateur auquel le rôle a été attribué ou retiré.
- Informations relatives aux fichiers d'application exécutables détectés sur l'appareil client (nom, chemin, type de fichier et hachage ; liste des catégories auxquelles l'application est affectée ; catégorie KL à laquelle l'application est affectée ; groupe de confiance auquel l'application est affectée ; premier lancement du fichier ; nom et version du demande ; nom du fabricant de l'application ; informations sur le certificat qui a signé la demande : numéro de série, empreinte digitale, émetteur, objet, date d'émission, date d'expiration et clé publique).
- Informations sur la liste réseau des chaînes de développement des menaces : identifiant de la chaîne de développement des menaces, heure de création de la chaîne de développement des menaces sous forme d'horodatage, format de la chaîne de développement des menaces (texte ou archive), taille du corps de la chaîne de développement des menaces en octets.

Données fournies lorsque vous cliquez sur des liens depuis l'interface de l'application

Lorsque vous cliquez sur des liens à partir de l'interface de l'application Kaspersky Endpoint Security, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes :

- version complète de l'application ;
- paramètres régionaux de l'application ;
- ID de l'application (PID) ;
- nom du lien.

Données fournies lors de l'utilisation de Kaspersky Security Network

L'ensemble des données que Kaspersky Security Network transfère à Kaspersky dépend du mode d'utilisation de Kaspersky Security Network.

Le fichier ksn_license.<ID de la langue> qui contient le texte de la Déclaration de Kaspersky Security Network se trouve dans le kit de distribution de l'application.

Fourniture de données lors de l'utilisation de KSN en mode standard

Si vous utilisez Kaspersky Security Network en mode KSN de base (le commutateur **« Utilisation de Kaspersky Security Network (KSN) »** est activé et la case **« Utiliser le mode étendu de KSN »** est décochée dans la Web Console, l'option **« Mode KSN de base »** est sélectionnée dans la Console d'administration), en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement les informations suivantes à Kaspersky.

Fourniture de données lors de l'utilisation de KSN en mode étendu

Si vous utilisez Kaspersky Security Network en mode étendu de KSN (le commutateur **« Utilisation de Kaspersky Security Network (KSN) »** est activé et la case **« Utiliser le mode étendu de KSN »** est cochée dans la Web Console, l'option **« Mode étendu de KSN »** est sélectionnée dans la Console d'administration), en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement les informations suivantes à Kaspersky en plus des informations indiquées ci-dessus.

Fourniture de données lors de l'utilisation du mode étendu de KSN avec l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)

Si vous utilisez Kaspersky Endpoint Security dans le cadre de Kaspersky Endpoint Detection and Response Expert (on-premises), ainsi que Kaspersky Security Network en mode étendu, en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes, en plus de celles indiquées ci-dessus.

Fourniture de données lors de l'utilisation de Kaspersky Endpoint Security en mode standard et en mode Agent de Endpoint Detection and Response

Si vous utilisez Kaspersky Endpoint Security en mode standard ou en Mode Endpoint Detection and Response Agent, ainsi que Kaspersky Security Network en mode étendu, en acceptant les termes de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement à Kaspersky, en plus des informations mentionnées ci-dessus, les informations suivantes :

Données fournies lors de l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum

Données transmises avec les résultats d'exécution des tâches *Analyse IOC*

Kaspersky Endpoint Security transfère automatiquement les données sur les résultats d'exécution des tâches *Analyse IOC* vers Kaspersky Security Center.

Les données des résultats d'exécution des tâches *Analyse IOC* peuvent contenir les informations suivantes :

- Informations réseau :
  - Adresse IP du tableau du protocole de résolution d'adresse (Address Resolution Protocol) ;
  - adresse MAC du tableau du protocole de résolution d'adresse ;
  - type et nom de l'enregistrement DNS ;
  - Adresse IP de l'appareil protégé
  - Adresse MAC de l'appareil protégé
  - adresse IP et port de connexion à distance ;
  - adresse IP de la carte réseau locale ;
  - numéro du port ouvert sur l'adaptateur local ;
  - numéro du protocole selon la norme IANA (Internet Assigned Numbers Authority).
- Informations relatives aux processus :
  - Nom du processus
  - Arguments du processus
  - chemin d'accès au fichier exécutable du processus ;
  - identifiant de processus (PID) ;
  - ID du processus parent ;
  - le nom de l'utilisateur qui a démarré le processus ;
  - Date et heure de démarrage du processus
- Informations sur les services :
  - Nom du service
  - Description du service
  - Chemin et nom du fichier exécutable du service
  - identifiant de service ;
  - type de service (pilote du noyau, adaptateur, etc.) ;
  - État du service
  - mode de démarrage du service ;
  - nom de l'utilisateur sous lequel le service est exécuté.

- Informations sur le système de fichiers :
  - Nom du volume
  - Lettre du volume
  - Type de volume
- Informations sur le système d'exploitation :
  - nom et version du système d'exploitation ;
  - Nom du réseau de l'appareil protégé
  - domaine ou groupe auquel appartient l'appareil.
- Informations sur l'activité Web :
  - Nom du navigateur
  - Version du navigateur
  - heure du dernier accès à la ressource Web ;
  - adresse Web de la requête HTTP ;
  - nom de l'utilisateur qui a effectué la requête HTTP ;
  - nom du processus qui a effectué la requête HTTP ;
  - chemin d'accès au fichier exécutable du processus qui a effectué la requête HTTP ;
  - ID du processus qui a effectué la requête HTTP ;
  - adresse Web de la source de la requête HTTP ;
  - adresse Web de la ressource demandée ;
  - agent utilisateur de la requête web traitée (HTTP User-Agent) ;
  - Temps d'exécution de la demande HTTP
  - identifiant unique du processus qui a effectué la requête HTTP.

Données permettant de créer une chaîne de développement de menaces

Les données permettant de créer une chaîne de développement de menaces peuvent contenir les informations suivantes :

- Informations générales sur l'alerte :
  - date et heure de l'alerte ;
  - Nom de l'objet
  - Mode d'analyse
  - état de la dernière activité associée à l'alerte ;
  - raison de l'échec du traitement de l'alerte.
- Informations concernant l'objet traité :
  - ID de processus ;
  - ID du processus parent ;
  - identifiant du fichier du processus ;
  - ligne de commande du processus ;
  - le nom de l'utilisateur qui a démarré le processus ;
  - identifiant de la session dans laquelle le processus s'exécute ;
  - type de session dans laquelle le processus s'exécute ;
  - niveau d'intégrité du processus traité ;
  - appartenance de l'utilisateur à des groupes privilégiés ;
  - identifiant de l'objet traité ;
  - Nom complet de l'objet traité
  - identifiant de l'appareil protégé ;
  - nom complet de l'objet (fichier local ou adresse Web) ;
  - hachages MD5 et SHA256 de l'objet traité ;
  - Type d'objet traité
  - date de création et dernière modification de l'objet ;
  - taille de l'objet en cours de traitement ;

- attributs de fichier d'un objet en cours de traitement ;
- informations sur l'organisation qui a signé l'objet ;
- résultat de la vérification du certificat numérique de l'objet ;
- Identifiant de sécurité (SID) de l'objet
- identifiant de fuseau horaire de l'objet ;
- adresse Web de téléchargement de l'objet (fichiers uniquement) ;
- Nom de l'application qui a téléchargé le fichier
- sommes de hachage MD5 et SHA256 de l'application qui a téléchargé le fichier ;
- Nom de l'application qui a modifié le fichier pour la dernière fois
- hachages MD5 et SHA256 de l'application qui a modifié le fichier en dernier lieu ;
- nombre de démarrages de l'objet traité ;
- date et heure du premier lancement de l'objet ;
- identifiant unique du fichier ;
- nom complet du fichier (fichier local ou adresse Web) ;
- Adresse Web de la demande Web traitée
- Source des liens de la requête web traitée (référent HTTP)
- Agent utilisateur de la demande Web traitée
- type de requête Web traitée (GET ou POST) ;
- Port IP local de la demande Web traitée
- Port IP distant de la demande Web traitée
- Sens de connexion (entrant ou sortant) de la demande Web traitée
- ID du processus dans lequel le code malveillant a été injecté.

Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response (KATA)

Lorsque Kaspersky Endpoint Security est intégré avec Kaspersky Endpoint Detection and Response (KATA), un module de la solution Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security stocke les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs dotés du module Central Node qui assurent l'interaction avec Kaspersky Endpoint Detection and Response (KATA) (ci-après également *serveurs KATA*) .
- clé publique du certificat du serveur pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA) ;
- Certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
- Identifiants d'authentification sur le serveur proxy.
- paramètres de fréquence de synchronisation avec le serveur KATA et paramètres de transfert de données vers le serveur KATA ;
- État de la connexion avec le serveur KATA et informations sur les erreurs de certificat client et de certificat serveur.
- Paramètres des tâches reçues des serveurs KATA :
  - Paramètres de la programmation du lancement d'une tâche
  - Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
  - Versions des paramètres
  - Type de lancement des services.
  - Noms des services.
  - Ligne de commande de lancement des processus avec les arguments.
  - Hachages MD5 et SHA256 des objets.
  - Chemins d'accès aux objets.
  - Fichiers IOC
- Paramètres d'isolation qui empêcheront l'appareil de communiquer avec d'autres appareils autres que ceux spécifiés dans les exclusions.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA), l'application Kaspersky Endpoint Security enregistre et peut transférer les données suivantes vers le serveur KATA :

- Données des requêtes de synchronisation vers le module EDR Expert (on-premises) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
- Données extraites des requêtes au module EDR Expert (on-premises) dans les rapports sur les résultats de tâche :
  - Adresse IP de l'appareil.
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Adresse MAC de l'appareil.
  - Erreurs d'exécution de tâche et codes de retour
  - États d'achèvement des tâches
  - Temps d'exécution de la tâche
  - Versions des paramètres d'exécution de la tâche.
  - Informations sur les processus lancés ou arrêtés sur l'appareil à la demande du serveur : PID et UniquePID, code d'erreur, hash MD5 et SHA-256 des objets
  - Fichiers demandés par le serveur
  - Données sur les erreurs d'obtention d'informations sur les objets : le nom complet de l'objet lors du traitement duquel une erreur s'est produite ; code d'erreur.
  - État de l'application d'isolement du réseau.

- Pour les indicateurs IOC, les résultats de la recherche sont renvoyés (si chaque indicateur a fonctionné ou non ; objets trouvés et informations sur la branche de l'indicateur qui a fonctionné).
- Pour les objets qui déclenchent des indicateurs IOC, différentes valeurs sont renvoyées selon le type d'indicateurs :
  - ArpEntry : adresse IP de la table ARP (y compris ipv6), adresse physique de la table ARP.
  - Fichier : hachage MD5 du fichier, hachage SHA-256 du fichier, nom complet du fichier (y compris le chemin), taille du fichier.
  - Port : adresse IP distante et port avec lequel une connexion a été établie au moment de la vérification ; Adresse IP et port de l'adaptateur local ; type de protocole (TCP, UDP, IP, RAWIP).
  - Processus : nom du processus ; arguments de processus ; chemin d'accès au fichier de processus ; PID système du processus ; PID système du processus parent ; le nom de l'utilisateur au nom duquel le processus est exécuté ; date et heure de début du processus.
  - SystemInfo : nom du système d'exploitation, version du système d'exploitation, nom réseau d'un appareil sans domaine, domaine ou groupe de travail.
  - User : nom d'utilisateur.
- Pour les objets mis en quarantaine :
  - Chemin du fichier
  - Taille du fichier
  - ID du fichier qui lui est attribué lors de la mise en quarantaine.
  - Indicateur concernant la suppression du fichier d'origine.
- Pour les fichiers reçus depuis la quarantaine :
  - ID du fichier qui lui est attribué lors de la mise en quarantaine.
- Pour les lancements interdits des fichiers exécutables ou des scripts :
  - Identifiant du processus
  - ID du processus parent ;
  - ID système.
  - ID de session de connexion au système.
  - État du processus
  - Date et heure de l'interception du lancement.

- Pour l'ouverture interdite de documents à l'aide des applications Office :
  - Identifiant du processus
  - ID du fichier.
  - Date et heure de l'interception du lancement.
- Données sur les fichiers :
  - identifiant unique du fichier ;
  - Hachage MD5 de l'objet
  - Contenu du fichier.
- Données dans les paquets de télémétrie :
  - Données sur les fichiers :
    - identifiant unique du fichier ;
    - Chemin du fichier
    - Nom du fichier
    - Taille du fichier
    - Attributs du fichier
    - Date et heure de création du fichier.
    - Date et heure de la dernière modification du fichier.
    - Hachages MD5 et SHA256 de l'objet
    - Informations sur l'utilisateur et le groupe propriétaire du fichier (nom et identifiant).
  - Données sur les processus en cours :
    - identifiant du fichier du processus ;
    - Identifiant du processus
    - Paramètres de lancement du processus.
    - Identifiant de la session.
    - Date et heure de démarrage du processus
    - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).

- Informations sur le processus accédant à la mémoire d'un autre processus :
  - Identifiant du processus
  - Méthode et adresse d'injection (injection).
  - Ligne de commande de modification des processus avec les arguments.
  - Arguments de l'appel système du processus
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Version des bases de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.
  - Identifiant unique du fichier de menace.
- Données de modification des fichiers :
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur les modifications apportées au système :
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur la connexion de l'utilisateur :
  - Identifiant de la session.
  - Informations sur l'utilisateur (nom et identifiant).
  - Adresse IP de l'appareil à partir duquel la session a été établie.
- Données sur la fin des processus : identifiant unique du processus.
- Informations sur le chargement de la bibliothèque dans l'espace d'adressage du processus : identifiant de la bibliothèque chargée.

- Informations sur l'établissement d'une connexion réseau :
  - Adresse IP locale.
  - Adresse IP à distance.
  - Sens de connexion.
  - Protocole
- Informations sur le processus qui « écoute » les connexions réseau externes sur un port spécifique :
  - Adresse locale (port et adresse IP).
  - Protocole
- Informations sur l'accès au serveur DNS :
  - Le nom de domaine de la ressource demandée.
  - Adresse IP de la ressource demandée.
  - Adresse IP du serveur DNS
  - Type de demande.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response Expert (on-premises)

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Liste des serveurs pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- Clé publique du certificat du serveur assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- Certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- Identifiants d'authentification sur le serveur proxy.
- Paramètres de fréquence de synchronisation avec le serveur assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), et paramètres de transfert des données pour ce serveur.
- État de la connexion au serveur qui gère l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), et informations sur les erreurs de certificat client et de certificat serveur.

- Paramètres des tâches reçues des serveurs assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) :
  - Paramètres de la programmation du lancement d'une tâche
  - Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
  - Versions des paramètres
  - Type de lancement des services.
  - Noms des services.
  - Ligne de commande de lancement des processus avec les arguments.
  - Hachages MD5 et SHA256 des objets.
  - Chemins d'accès aux objets.
  - Fichiers IOC
- Paramètres d'isolation qui empêcheront l'appareil de communiquer avec d'autres appareils autres que ceux spécifiés dans les exclusions.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises), l'application enregistre et peut transmettre les données suivantes au serveur d'intégration :

- Informations pour les requêtes de synchronisation vers le module EDR Expert (on-premises) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
- Informations provenant des requêtes au module EDR Expert (on-premises) dans les rapports d'exécution des tâches :
  - Adresse IP de l'appareil.
  - Identifiant unique.

- Partie essentielle de l'adresse Internet du serveur.
- Adresse MAC de l'appareil.
- Erreurs d'exécution de tâche et codes de retour
- États d'achèvement des tâches
- Temps d'exécution de la tâche
- Versions des paramètres d'exécution de la tâche.
- Informations sur les processus lancés ou arrêtés sur l'appareil à la demande du serveur : PID et UniquePID, code d'erreur, hash MD5 et SHA-256 des objets
- Fichiers demandés par le serveur
- Données sur les erreurs d'obtention d'informations sur les objets : le nom complet de l'objet lors du traitement duquel une erreur s'est produite ; code d'erreur.
- État de l'application d'isolement du réseau.
- Pour les indicateurs IOC, les résultats de la recherche sont renvoyés (si chaque indicateur a fonctionné ou non ; objets trouvés et informations sur la branche de l'indicateur qui a fonctionné).
- Pour les règles YARA, les résultats de recherche sont renvoyés (déclenchement ou non de la règle, objets trouvés et informations sur la règle déclenchée).
- Les objets qui ont déclenché les indicateurs IoC, les règles Yara, renvoient des valeurs différentes selon le type :
  - ArpEntry : adresse IP de la table ARP (y compris ipv6), adresse physique de la table ARP.
  - Fichier : hachage MD5 du fichier, hachage SHA-256 du fichier, nom complet du fichier (y compris le chemin), taille du fichier.
  - Port : adresse IP distante et port avec lequel une connexion a été établie au moment de la vérification ; Adresse IP et port de l'adaptateur local ; type de protocole (TCP, UDP, IP, RAWIP).
  - Processus : nom du processus ; arguments de processus ; chemin d'accès au fichier de processus ; PID système du processus ; PID système du processus parent ; le nom de l'utilisateur au nom duquel le processus est exécuté ; date et heure de début du processus.
  - SystemInfo : nom du système d'exploitation, version du système d'exploitation, nom réseau d'un appareil sans domaine, domaine ou groupe de travail.
  - User : nom d'utilisateur.
- Pour les objets mis en quarantaine :
  - Chemin du fichier
  - Taille du fichier

- Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.
- Indicateur concernant la suppression du fichier d'origine.

- Pour les fichiers reçus, restaurés ou supprimés de la quarantaine :
  - Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.
- Pour les lancements interdits des fichiers exécutables ou des scripts :
  - Identifiant du processus
  - ID du processus parent ;
  - ID système.
  - ID de session de connexion au système.
  - État du processus
  - Date et heure de l'interception du lancement.
- Pour l'ouverture interdite de documents à l'aide des applications Office :
  - Identifiant du processus
  - ID du fichier.
  - Date et heure de l'interception du lancement.
- Liste des fichiers dans le répertoire spécifié :
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Taille du fichier
  - Type de fichiers
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Métadonnées des fichiers.
  - Nombre de liens physiques vers le fichier.
  - Dates de création, de modification et de dernier accès aux fichiers.

- Liste des processus en cours d'exécution sur l'appareil :
  - Nom du processus
  - Heure de début du processus.
  - État du processus
  - Identifiant du processus (PID) et identifiant du processus parent.
  - Répertoire de travail actuel.
  - Paramètres de lancement du processus.
  - Variables d'environnement.
  - chemin d'accès au fichier exécutable du processus ;
  - Identifiant de session de l'utilisateur ayant lancé le processus.
  - Identifiant de l'utilisateur et du groupe ayant lancé le processus.
  - Identifiant de l'utilisateur et du groupe avec lesquels le processus a accès aux fichiers et aux ressources du système.
- Liste des points d'auto-démarrage :
  - Type de point d'auto-démarrage.
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Dates de création, de modification et de dernier accès aux fichiers.
- Image mémoire du processus :
  - Nom du processus
  - Chemin d'accès complet au fichier.
  - fichier de vidage du processus.
  - Taille du fichier de vidage du processus.
- Image mémoire de l'appareil : fichier de vidage de la mémoire vive de l'appareil.
- Image disque de l'appareil.

- Données sur les fichiers :
  - identifiant unique du fichier ;
  - Hachage MD5 de l'objet
  - Contenu du fichier.
- Données dans les paquets de télémétrie :
  - Données d'événements de télémétrie :
    - ID de l'événement.
    - Numéro de séquence de l'événement dans la séquence des paquets de télémétrie envoyés.
    - Type d'événement.
    - Heure de l'événement.
  - Les informations sur l'appareil protégé :
    - Nom de l'appareil protégé.
    - Identifiant de l'appareil protégé dans Kaspersky Security Center.
    - Identifiant de l'appareil protégé dans Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Nom, version et famille du système d'exploitation installé sur l'appareil protégé.
    - Heures de démarrage et d'arrêt du système d'exploitation installé sur l'appareil protégé.
  - Données sur les fichiers :
    - identifiant unique du fichier ;
    - Chemin du fichier
    - Nom du fichier
    - Taille du fichier
    - Attributs du fichier
    - Date et heure de création du fichier.
    - Date et heure de la dernière modification du fichier.
    - Hachages MD5 et SHA256 de l'objet
    - Informations sur l'utilisateur et le groupe propriétaire du fichier (nom et identifiant).

- Données sur les processus en cours :
  - identifiant du fichier du processus ;
  - Identifiant du processus
  - Paramètres de lancement du processus.
  - Identifiant de la session.
  - Date et heure de démarrage du processus
  - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).
- Informations sur le processus accédant à la mémoire d'un autre processus :
  - Identifiant du processus
  - Méthode et adresse d'injection (injection).
  - Ligne de commande de modification des processus avec les arguments.
  - Arguments de l'appel système du processus
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Date de publication et version des bases de données de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.
  - Identifiant unique du fichier de menace.
- Données de modification des fichiers :
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur les modifications apportées au système :
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.

- Informations sur la connexion de l'utilisateur :
  - Identifiant de la session.
  - Informations sur l'utilisateur (nom et identifiant).
  - Adresse IP de l'appareil à partir duquel la session a été établie.
- Données sur la fin des processus : identifiant unique du processus.
- Informations sur le chargement de la bibliothèque dans l'espace d'adressage du processus : identifiant de la bibliothèque chargée.
- Informations sur l'établissement et la fin d'une connexion réseau :
  - Adresse IP locale.
  - Adresse IP à distance.
  - Sens de connexion.
  - Protocole
  - Heure d'établissement de la connexion
  - Heure de fin de la connexion
  - Durée de la connexion
  - Octets envoyés pendant la connexion
  - Octets reçus pendant la connexion
- Informations sur le processus qui « écoute » les connexions réseau externes sur un port spécifique :
  - Adresse locale (port et adresse IP).
  - Protocole
- Informations sur l'accès au serveur DNS :
  - Le nom de domaine de la ressource demandée.
  - Adresse IP de la ressource demandée.
  - Adresse IP du serveur DNS
  - Type de demande.
- Informations sur les appareils externes connectés :
  - Type d'opération (connexion de l'appareil).
  - Type d'appareil.

- Identifiant unique de l'appareil.
- Nom de l'appareil
- Chemin d'accès à l'appareil.

- Informations sur l'application et ses modules :
  - Version de l'application.
  - Heures d'installation, de démarrage, d'arrêt et de suppression de l'application.
  - Initiateur de l'action de l'application.
  - Motif de l'arrêt de l'application en cas d'arrêt anormal.
  - Codes de retour en cas d'arrêt anormal.
- Informations sur l'interaction avec les planificateurs de tâches (création et suppression des tâches) :
  - Nom de la tâche.
  - Chemin d'accès à la commande exécutée conformément à la planification.
  - Planifier l'exécution de la tâche.
  - Nom du compte utilisateur ayant créé la tâche.
  - Nom du compte sous lequel la tâche est exécutée.
  - Nom du compte utilisateur ayant supprimé la tâche.
- Informations sur la création, la suppression et la modification des services :
  - Nom du service (y compris le précédent s'il a été modifié).
  - Type de service (y compris le précédent s'il a été modifié).
  - Chemin d'accès au fichier exécutable (y compris le précédent s'il a été modifié).
  - Dépendance du service (y compris les précédentes s'il a été modifié).
  - Nom du compte sous lequel le service s'exécute (y compris le précédent s'il a été modifié).
  - Nom d'affichage du service (y compris le nom précédent s'il a été modifié).
  - Nom du compte utilisateur ayant créé, supprimé ou modifié le service.
  - Indicateur de suppression différée.
- Informations de saisie dans la console :
  - Identifiant et type du processus ayant initié la saisie dans la console.
  - Contenu de saisie dans la console.

- Informations sur les appareils montés :
  - Nom de système du volume.
  - Points de montage.
- Informations sur les modifications de la mémoire du processus :
  - Arguments de l'appel système du processus
  - Informations sur le processus ayant effectué l'injection de code et son processus parent.
    - Identifiant du processus et identifiant unique du processus et du processus parent.
    - Ligne de commande à partir de laquelle le processus et le processus parent ont été lancés.
    - Variables d'environnement de processus.
    - Type de compte utilisateur sous lequel le processus et le processus parent ont été lancés.
    - Appel système utilisé pour créer le processus.
    - Identifiant de l'utilisateur et du groupe ayant lancé le processus.
    - Nom et nom complet du processus et du processus parent.
    - Chemin complet du processus et du processus parent.
    - Hachages MD5 et SHA256 du processus et du processus parent.
    - Identifiant de la session.
    - Nom, nom de domaine et identifiant de l'utilisateur ayant lancé le processus et le processus parent.
  - Informations sur le processus par lequel le processus ayant injecté le code a été chargé.
    - Identifiant unique du processus ayant servi à charger le processus.
    - Nom et chemin complet du fichier ayant servi à charger le processus.
    - Chemin complet du processus ayant servi à charger le processus.
    - Hachage MD5 du processus ayant lancé le processus.
  - Informations sur le processus initiateur.
    - Identifiant et identifiant unique du processus initiateur.
    - Ligne de commande du processus initiateur.
    - Nom et nom de domaine de l'utilisateur ayant lancé le processus initiateur.
    - Nom et nom complet du processus initiateur.

- Chemin d'accès complet au processus initiateur.
- Hachages MD5 et SHA256 du processus initiateur.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response Expert (cloud)

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (cloud), l'application Kaspersky Endpoint Security enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Liste des serveurs assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).
- Adresses des tunnels des serveurs de télémétrie et de réponse pour Kaspersky Endpoint Detection and Response Expert (cloud).
- Certificat serveur pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).
- Certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud).
- Paramètres de fréquence de synchronisation avec le serveur assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud), et paramètres de transmission des données pour ce serveur.
- L'état de la connexion au serveur qui assure l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud), ainsi que des informations sur les erreurs de certificat client et de certificat serveur.
- Paramètres des tâches reçues des serveurs assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (cloud) :
  - Paramètres de la programmation du lancement d'une tâche
  - Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
  - Versions des paramètres
  - Type de lancement des services.
  - Noms des services.
  - Ligne de commande de lancement des processus avec les arguments.
  - Hachages MD5 et SHA256 des objets.
  - Chemins d'accès aux objets.
  - Fichiers IOC
- Paramètres d'isolation qui empêcheront l'appareil de communiquer avec d'autres appareils autres que ceux spécifiés dans les exclusions.

Lorsque l'application Kaspersky Endpoint Security est intégrée à Kaspersky Endpoint Detection and Response Expert (cloud), l'application enregistre et peut transmettre les données suivantes au serveur d'intégration :

- Données des requêtes de synchronisation vers le module EDR Expert (cloud) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
- Données extraites des requêtes au module EDR Expert (cloud) dans les rapports sur les résultats de tâche :
  - Adresse IP de l'appareil.
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Adresse MAC de l'appareil.
  - Erreurs d'exécution de tâche et codes de retour
  - États d'achèvement des tâches
  - Temps d'exécution de la tâche
  - Versions des paramètres d'exécution de la tâche.
  - Informations sur les processus lancés sur l'appareil à la demande du serveur :
    - Code de fin du processus
    - Identifiant unique du fichier de sortie standard du processus.
    - Identifiant unique du fichier d'erreur standard du processus.

- Informations sur les processus lancés ou arrêtés sur l'appareil à la demande du serveur :
  - PID (identifiant système du processus).
  - UniquePID (identifiant unique du processus)
  - Code d'erreur
- Copie du fichier demandé par le serveur, ainsi que le chemin d'accès au fichier et son identifiant.
- Indicateur de suppression du fichier après le redémarrage du système d'exploitation.
- Données sur les erreurs d'obtention d'informations sur les objets : le nom complet de l'objet lors du traitement duquel une erreur s'est produite ; code d'erreur.
- État de l'application d'isolement du réseau.
- Pour les indicateurs IOC, les résultats de la recherche sont renvoyés (si chaque indicateur a fonctionné ou non ; objets trouvés et informations sur la branche de l'indicateur qui a fonctionné).
- Pour les objets dans lesquels des IoC ont été détectés, différentes valeurs sont renvoyées selon le type d'indicateur :
  - ArpEntry : adresse IP de la table ARP (y compris ipv6), adresse physique de la table ARP.
  - Fichier : hachage MD5 du fichier, hachage SHA-256 du fichier, nom complet du fichier (y compris le chemin), taille du fichier.
  - Port : adresse IP distante et port avec lequel une connexion a été établie au moment de la vérification ; Adresse IP et port de l'adaptateur local ; type de protocole (TCP, UDP, IP, RAWIP).
  - Processus : nom du processus ; arguments de processus ; chemin d'accès au fichier de processus ; PID système du processus ; PID système du processus parent ; le nom de l'utilisateur au nom duquel le processus est exécuté ; date et heure de début du processus.
  - SystemInfo : nom du système d'exploitation, version du système d'exploitation, nom réseau d'un appareil sans domaine, domaine ou groupe de travail.
  - User : nom d'utilisateur.
- Pour les objets mis en quarantaine :
  - Chemin du fichier
  - Taille du fichier
  - Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.
  - Indicateur concernant la suppression du fichier d'origine.
- Pour les fichiers reçus, restaurés ou supprimés de la quarantaine :
  - Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.

- Pour les lancements interdits des fichiers exécutables ou des scripts :
  - Identifiant du processus
  - ID du processus parent ;
  - ID système.
  - ID de session de connexion au système.
  - État du processus
  - Date et heure de l'interception du lancement.
- Pour l'ouverture interdite de documents à l'aide des applications Office :
  - Identifiant du processus
  - ID du fichier.
  - Date et heure de l'interception du lancement.
- Liste des fichiers dans le répertoire spécifié :
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Taille du fichier
  - Type de fichiers
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Métadonnées des fichiers.
  - Nombre de liens physiques vers le fichier.
  - Dates de création, de modification et de dernier accès aux fichiers.
- Liste des processus en cours d'exécution sur l'appareil :
  - Nom du processus
  - Heure de début du processus.
  - État du processus
  - Identifiant du processus (PID) et identifiant du processus parent.
  - Répertoire de travail actuel.

- Paramètres de lancement du processus.
- Variables d'environnement.
- chemin d'accès au fichier exécutable du processus ;
- Identifiant de session de l'utilisateur ayant lancé le processus.
- Identifiant de l'utilisateur et du groupe ayant lancé le processus.
- Identifiant de l'utilisateur et du groupe avec lesquels le processus a accès aux fichiers et aux ressources du système.

- Liste des points d'auto-démarrage :
  - Type de point d'auto-démarrage.
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Dates de création, de modification et de dernier accès aux fichiers.
  - Hachage MD5 et hachage SHA-256 du fichier exécutable ou du module chargeable.
- Image mémoire du processus :
  - Nom du fichier d'image mémoire du processus.
  - Chemin d'accès complet au fichier.
  - Identifiant unique du fichier d'image mémoire du processus.
  - Taille du fichier d'image mémoire du processus.
- Image mémoire de l'appareil :
  - Date et heure auxquelles le vidage a commencé.
  - Chemin d'accès complet au fichier de vidage
  - Taille du fichier d'image mémoire de l'appareil.
- Image disque de l'appareil :
  - Date et heure auxquelles le vidage a commencé.
  - Tableau des chemins d'accès complets aux fichiers de vidage

- Taille du fichier d'image disque de l'appareil.
- Disque logique.
- Disque physique.

- Données dans les paquets de télémétrie :
  - Données d'événements de télémétrie :
    - ID de l'événement.
    - Numéro de séquence de l'événement dans la séquence des paquets de télémétrie envoyés.
    - Type d'événement.
    - Heure de l'événement.
  - Les informations sur l'appareil protégé :
    - Nom de l'appareil protégé.
    - Identifiant de l'appareil protégé dans Kaspersky Security Center.
    - Identifiant de l'appareil protégé dans Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Nom, version et famille du système d'exploitation installé sur l'appareil protégé.
    - Heures de démarrage et d'arrêt du système d'exploitation installé sur l'appareil protégé.
  - Données sur les fichiers :
    - identifiant unique du fichier ;
    - Chemin du fichier
    - Nom du fichier
    - Taille du fichier
    - Attributs du fichier
    - Date et heure de création du fichier.
    - Date et heure de la dernière modification du fichier.
    - Hachages MD5 et SHA256 de l'objet
    - Informations sur l'utilisateur et le groupe propriétaire du fichier (nom et identifiant).
  - Données sur les processus en cours :
    - identifiant du fichier du processus ;
    - Identifiant du processus

- Paramètres de lancement du processus.
- Identifiant de la session.
- Date et heure de démarrage du processus
- Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).

- Informations sur le processus accédant à la mémoire d'un autre processus :
  - Identifiant du processus
  - Méthode et adresse d'injection (injection).
  - Ligne de commande de modification des processus avec les arguments.
  - Arguments de l'appel système du processus
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Date de publication et version des bases de données de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.
  - Identifiant unique du fichier de menace.
- Données de modification des fichiers :
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur les modifications apportées au système :
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur la connexion de l'utilisateur :
  - Identifiant de la session.
  - Informations sur l'utilisateur (nom et identifiant).
  - Adresse IP de l'appareil à partir duquel la session a été établie.

- Données sur la fin des processus : identifiant unique du processus.
- Informations sur le chargement de la bibliothèque dans l'espace d'adressage du processus : identifiant de la bibliothèque chargée.
- Informations sur l'établissement et la fin d'une connexion réseau :
  - Adresse IP locale.
  - Adresse IP à distance.
  - Sens de connexion.
  - Protocole
  - Heure d'établissement de la connexion
  - Heure de fin de la connexion
  - Durée de la connexion
  - Octets envoyés pendant la connexion
  - Octets reçus pendant la connexion
- Informations sur le processus qui « écoute » les connexions réseau externes sur un port spécifique :
  - Adresse locale (port et adresse IP).
  - Protocole
- Informations sur l'accès au serveur DNS :
  - Le nom de domaine de la ressource demandée.
  - Adresse IP de la ressource demandée.
  - Adresse IP du serveur DNS
  - Type de demande.
- Informations sur les appareils externes connectés :
  - Type d'opération (connexion de l'appareil).
  - Type d'appareil.
  - Identifiant unique de l'appareil.
  - Nom de l'appareil
  - Chemin d'accès à l'appareil.

- Informations sur l'application et ses modules :
  - Version de l'application.
  - Heures d'installation, de démarrage, d'arrêt et de suppression de l'application.
  - Initiateur de l'action de l'application.
  - Motif de l'arrêt de l'application en cas d'arrêt anormal.
  - Codes de retour en cas d'arrêt anormal.
- Informations sur l'interaction avec les planificateurs de tâches (création et suppression des tâches) :
  - Nom de la tâche.
  - Chemin d'accès à la commande exécutée conformément à la planification.
  - Planifier l'exécution de la tâche.
  - Nom du compte utilisateur ayant créé la tâche.
  - Nom du compte sous lequel la tâche est exécutée.
  - Nom du compte utilisateur ayant supprimé la tâche.
- Informations sur la création, la suppression et la modification des services :
  - Nom du service (y compris le précédent s'il a été modifié).
  - Type de service (y compris le précédent s'il a été modifié).
  - Chemin d'accès au fichier exécutable (y compris le précédent s'il a été modifié).
  - Dépendance du service (y compris les précédentes s'il a été modifié).
  - Nom du compte sous lequel le service s'exécute (y compris le précédent s'il a été modifié).
  - Nom d'affichage du service (y compris le nom précédent s'il a été modifié).
  - Nom du compte utilisateur ayant créé, supprimé ou modifié le service.
  - Indicateur de suppression différée.
- Informations de saisie dans la console :
  - Identifiant et type du processus ayant initié la saisie dans la console.
  - Contenu de saisie dans la console.
- Informations sur les appareils montés :
  - Nom de système du volume.
  - Points de montage.

- Informations sur les modifications de la mémoire du processus :
  - Arguments de l'appel système du processus
  - Informations sur le processus ayant effectué l'injection de code et son processus parent.
    - Identifiant du processus et identifiant unique du processus et du processus parent.
    - Ligne de commande à partir de laquelle le processus et le processus parent ont été lancés.
    - Variables d'environnement de processus.
    - Type de compte utilisateur sous lequel le processus et le processus parent ont été lancés.
    - Appel système utilisé pour créer le processus.
    - Identifiant de l'utilisateur et du groupe ayant lancé le processus.
    - Nom et nom complet du processus et du processus parent.
    - Chemin complet du processus et du processus parent.
    - Hachages MD5 et SHA256 du processus et du processus parent.
    - Identifiant de la session.
    - Nom, nom de domaine et identifiant de l'utilisateur ayant lancé le processus et le processus parent.
  - Informations sur le processus par lequel le processus ayant injecté le code a été chargé.
    - Identifiant unique du processus ayant servi à charger le processus.
    - Nom et chemin complet du fichier ayant servi à charger le processus.
    - Chemin complet du processus ayant servi à charger le processus.
    - Hachage MD5 du processus ayant lancé le processus.
  - Informations sur le processus initiateur.
    - Identifiant et identifiant unique du processus initiateur.
    - Ligne de commande du processus initiateur.
    - Nom et nom de domaine de l'utilisateur ayant lancé le processus initiateur.
    - Nom et nom complet du processus initiateur.
    - Chemin d'accès complet au processus initiateur.
    - Hachages MD5 et SHA256 du processus initiateur.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec Kaspersky Network Detection and Response (KATA)

Lorsque Kaspersky Endpoint Security est intégré avec le module Kaspersky Network Detection and Response (KATA), un module de la solution Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security stocke les informations de service suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs NDR.
- Clé publique du certificat du serveur pour l'intégration avec Kaspersky Network Detection and Response (KATA).
- Certificat client pour l'intégration avec Kaspersky Network Detection and Response (KATA).
- Identifiants d'authentification sur le serveur proxy.
- paramètres de fréquence de synchronisation avec le serveur NDR et paramètres de transfert de données vers le serveur NDR ;
- État de la connexion avec le serveur NDR et informations sur les erreurs de certificat client et de certificat serveur.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Network Detection and Response (KATA), l'application Kaspersky Endpoint Security enregistre et transmet les données suivantes au serveur NDR :

- Données des demandes de synchronisation vers le serveur NDR :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom, famille et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
  - Modèle et fabricant de l'appareil de l'utilisateur.

- Données dans les paquets de télémétrie :
  - Informations sur l'appareil et les utilisateurs :
    - Nom de l'appareil et heure sur l'appareil.
    - Nom, famille et version du système d'exploitation
    - Informations sur les interfaces réseau (description, liste des adresses IP avec masque de sous-réseau, adresse MAC, numéro de métrique, nom de domaine DNS, informations de routage, numéros de port d'écoute).
    - Identifiant interne unique de l'appareil
    - Noms d'utilisateur et identifiants.
    - Noms et identifiants des groupes d'utilisateurs.
  - Informations sur l'application Kaspersky Endpoint Security :
    - nom et version de l'application.
    - La date à laquelle l'application a été mise à jour pour la dernière fois.
    - Informations sur les clés de licence (numéro de série, type, période de validité de la licence, état de la clé)
    - Version des bases de l'application.
    - Liste des versions d'API prises en charge
  - Informations sur les connexions établies :
    - Adresse IP locale, port et adresse MAC
    - Adresse IP à distance, port et adresse MAC.
    - Adresse IP de la passerelle.
    - Type de protocole (par IANA), numéro de protocole et EtherType.
    - Nombre de paquets reçus et transmis.
  - Informations sur les fichiers traités :
    - Le nom et l'identifiant unique du fichier.
    - Type et taille du fichier.
    - Chemin d'accès complet à l'image du fichier.
    - Masque d'attributs du système de fichiers.
    - Heure à laquelle le fichier a été créé et modifié

- hash MD5 et SHA-256 de l'objet.
- Privilèges du fichier, y compris hérités et effectifs.

- Informations sur les processus en cours d'exécution et de fin :
  - UID et PID du processus.
  - Type de processus.
  - Identifiant de la session.
  - La commande à exécuter.
  - Variables d'environnement.
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Version des bases de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Unified Monitoring and Analysis Platform, l'application Kaspersky Endpoint Security enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs KUMA.
- Clé publique du certificat du serveur pour l'intégration avec Kaspersky Unified Monitoring and Analysis Platform (sauf dans le cas où le protocole UDP est utilisé pour se connecter au serveur KUMA).
- Certificat client pour l'intégration avec Kaspersky Unified Monitoring and Analysis Platform.
- Identifiants d'authentification sur le serveur proxy.

- paramètres de fréquence de synchronisation avec le serveur KUMA et paramètres de transfert de données vers le serveur KUMA ;
- État de la connexion avec le serveur KUMA et informations sur les erreurs de certificat client et de certificat serveur.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform, l'application Kaspersky Endpoint Security enregistre et transmet les données suivantes au serveur KUMA dans des paquets de télémétrie :

- Informations sur la modification des fichiers :
  - ID unique du fichier avant modification.
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Type et indicateur de l'opération sur le fichier.
  - Date et heure de la modification du fichier.
- Informations sur les processus en cours d'exécution et de fin :
  - identifiant du fichier du processus ;
  - UID et PID du processus.
  - Paramètres de lancement du processus.
  - Identifiant de la session.
  - Date et heure de démarrage du processus
  - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).
- Informations sur les événements dans le journal des événements :
  - date et heure de l'événement ;
  - UID du processus associé à l'événement.
  - Type d'événement et description.
  - Résultat d'exécution de l'opération.

Informations sur le code tiers

L'information sur le code tiers se trouve dans le fichier legal_notices.txt, situé dans le dossier d'installation de l'application.

Notice sur les marques de commerce

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash et Shockwave sont des marques ou des marques déposées d'Adobe aux États-Unis et/ou dans d'autres pays.

AMD64 est une marque commerciale ou une marque déposée d'Advanced Micro Devices, Inc.

Amazon est une marque commerciale d'Amazon.com, Inc. ou ses affiliés.

Arm est une marque déposée d'Arm Limited (ou de ses filiales) aux États-Unis et/ou dans d'autres pays.

AutoCAD est une marque ou une marque déposée aux États-Unis et/ou dans d'autres pays qui appartient à Autodesk, Inc. et/ou à ses filiales.

Borland est une marque ou une marque déposée de Borland Software Corporation.

dBase est une marque de dataBased Intelligence, Inc.

FireWire est une marque commerciale d'Apple Inc.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Ubuntu et LTS sont des marques de commerce déposées de Canonical Ltd.

XenServer est une marque déposée ou une marque commerciale de Cloud Software Group, Inc. et/ou filiales aux États-Unis et/ou dans d'autres pays.

Cloudflare, le logo Cloudflare et Cloudflare Workers sont des marques commerciales et/ou des marques déposées de Cloudflare, Inc. aux États-Unis et dans d'autres juridictions.

La marque verbale Grafana et le logo Grafana sont des marques déposées/marques de service ou des marques commerciales/marques de service de Coding Instinct AB aux États-Unis et dans d'autres pays et sont utilisés avec l'autorisation de Coding Instinct. Nous ne sommes pas affiliés, approuvés ou sponsorisés par Coding Instinct ou la communauté Grafana.

Docker et le logo Docker sont des marques de commerce ou des marques déposées de Docker, Inc. aux États-Unis et/ou dans d'autres pays. Docker, Inc. et d'autres parties peuvent également avoir des droits de marque de commerce dans d'autres termes utilisés dans le présent document.

Chrome, Chromium, Google Chrome et Google Public DNS sont des marques commerciales de Google LLC.

HUAWEI, EulerOS, FusionSphere sont des marques commerciales de Huawei Technologies Co., Ltd.

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

Microsoft, Microsoft Edge, Active Directory, Hyper-V, Outlook, Visual Basic, Visual FoxPro, Visual C++, PowerPoint, Excel, Internet Explorer, Windows et Windows Server sont des marques commerciales du groupe de sociétés Microsoft.

OpenStack est une marque déposée de la OpenStack Foundation aux États-Unis et dans d'autres pays.

Oracle, Java et JavaScript sont des marques déposées d'Oracle et/ou de ses filiales.

Python est une marque de commerce ou une marque déposée de la Python Software Foundation.

Red Hat Enterprise Linux, CentOS et Fedora sont des marques commerciales ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc.

Kubernetes est une marque déposée de The Linux Foundation aux États-Unis et dans d'autres pays.

Rocky Linux est une marque déposée de The Rocky Enterprise Software Foundation.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, sous licence exclusive de X/Open Company Limited.

Zabbix est une marque déposée de Zabbix SIA.